Instalar y configurar VMware ESXi

Actualización 3

VMware vSphere 8.0
VMware ESXi 8.0



Puede encontrar la documentación técnica más actualizada en el sitio web de VMware by Broadcom en:

https://docs.vmware.com/es/

VMware by Broadcom
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contenido

Acerca de instalar y configurar VMware ESXi

1

En el documento Instalar y configurar VMware ESXi, se describe cómo instalar y configurar VMware ESXi™.

En VMware, valoramos la inclusión. Para fomentar este principio en nuestros clientes y clientas, partners y comunidad interna, hemos actualizado esta guía para eliminar las instancias de lenguaje no inclusivo.

Audiencia prevista

El documento *Instalar y configurar VMware ESXi* está destinado a administradores experimentados que deseen instalar y configurar ESXi.

Esta información está escrita para administradores del sistema de Windows y Linux expertos que están familiarizados con la tecnología de máquina virtual y las operaciones de centro de datos. La información sobre el uso de Image Builder y VMware vSphere® Auto Deploy™ está escrita para administradores que tienen experiencia con Microsoft PowerShell y VMware vSphere® PowerCLI™.

Introducción a la instalación y configuración de vSphere

2

vSphere 8.0 ofrece varias opciones de instalación y configuración que definen la secuencia de tareas correspondiente.

Los dos componentes principales de vSphere son ESXi y vCenter Server. ESXi es la plataforma de virtualización en la que se crean y se ejecutan las máquinas virtuales y los dispositivos virtuales. vCenter Server es un servicio que actúa como administrador central de los hosts ESXi conectados en una red. vCenter Server permite agrupar y administrar los recursos de varios hosts.

Debe implementar vCenter Server Appliance, una máquina virtual preconfigurada y optimizada para ejecutar vCenter Server y los componentes de vCenter Server. Puede implementar la instancia de vCenter Server Appliance en hosts ESXi o instancias de vCenter Server.

Para obtener información detallada sobre el proceso de instalación de vCenter Server, consulte *Instalar y configurar vCenter Server*.

Lea los siguientes temas a continuación:

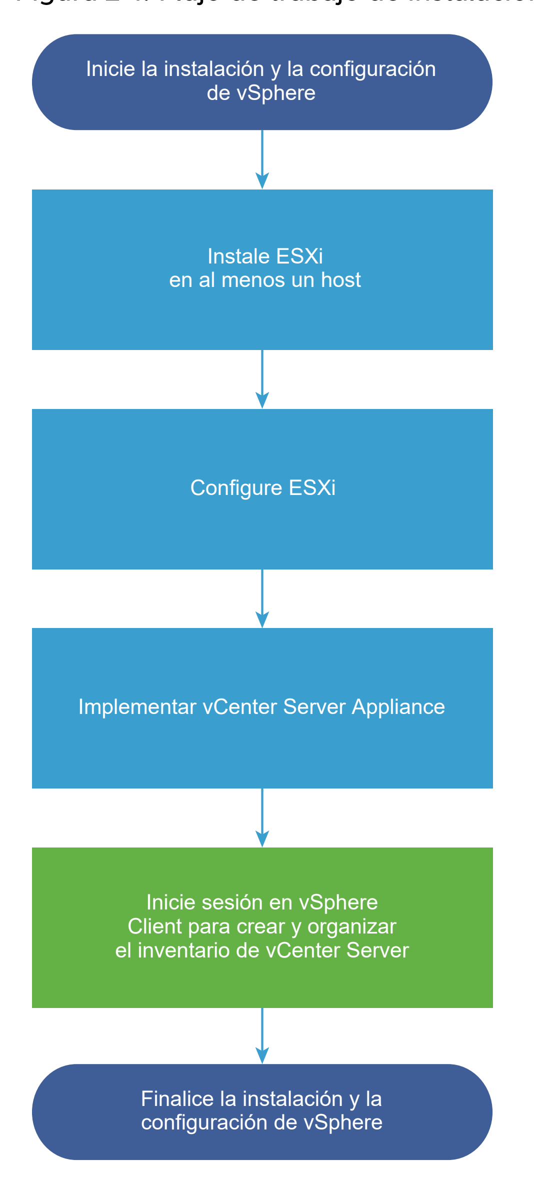
- Información general del proceso de instalación y configuración de vSphere
- Acerca de los modos de evaluación y con licencia de ESXi

Información general del proceso de instalación y configuración de vSphere

vSphere es un producto sofisticado con varios componentes que puede instalar y configurar. A fin de garantizar una implementación correcta de vSphere, comprenda la secuencia de las tareas requeridas.

La instalación de vSphere incluye las siguientes tareas:

Figura 2-1. Flujo de trabajo de instalación y configuración de vSphere



1 Lea las notas de la versión de vSphere.

2 Instale ESXi.

   a Compruebe que el sistema cumpla con los requisitos de hardware mínimos. Consulte Requisitos de ESXi.

   b Determine la opción de instalación de ESXi que se utilizará: interactiva, generada por script o mediante vSphere Auto Deploy.

   c Determine dónde desea ubicar y arrancar el instalador de ESXi. Consulte Opciones de medios para arrancar el instalador de ESXi. Si va a utilizar PXE para arrancar el instalador, compruebe que la infraestructura PXE de la red esté configurada correctamente. Consulte Arranque de red del instalador de ESXi.

d Cree una hoja de cálculo con la información que necesitará al instalar ESXi. Consulte Información obligatoria para instalar ESXi.

e Instale ESXi.

- Instalar ESXi de forma interactiva
- Instalación de ESXi generada por script

Nota También puede aprovisionar hosts ESXi con vSphere Auto Deploy, pero vSphere Auto Deploy se instala junto con vCenter Server. A fin de aprovisionar hosts ESXi con Auto Deploy, deberá instalar vCenter Server.

3 Ajuste la configuración de red y arranque de ESXi, la consola directa y otras opciones. Consulte Configurar ESXi y Después de instalar y configurar ESXi.

4 Considere la posibilidad de configurar un servidor de Syslog para inicio de sesión remoto, a fin de garantizar que haya almacenamiento de disco suficiente para los archivos de registro. La configuración del registro en un host remoto es especialmente importante para hosts con almacenamiento local limitado. Consulte Espacio libre necesario para registro del sistema y Configurar Syslog en hosts ESXi.

5 Instale vCenter Server.

Para información detallada, consulte la guía Instalar y configurar vCenter Server.

Acerca de los modos de evaluación y con licencia de ESXi

Puede utilizar el modo de evaluación para explorar un conjunto de características igual a la licencia de vSphere Enterprise Plus.

Puede utilizar el modo de evaluación para explorar el conjunto completo de funciones para los hosts ESXi. El modo de evaluación proporciona un conjunto de funciones equivalente a una licencia de vSphere Enterprise Plus. Antes de que finalice el modo de evaluación, debe asignar a sus hosts una licencia que admita todas las funciones en uso. Por ejemplo, en el modo de evaluación, puede utilizar la tecnología vSphere vMotion, la función vSphere HA, la característica vSphere DRS y otras características. Si desea continuar utilizando estas funciones, debe asignar una licencia que las admita.

La versión de los hosts ESXi Installable se instala siempre en el modo de evaluación. ESXi Embedded se ofrece preinstalado en el dispositivo de almacenamiento interno por parte de cada proveedor de hardware. Podría estar en el modo de evaluación o con licencia previa.

El período de evaluación es de 60 días y comienza cuando se enciende el host ESXi. En cualquier momento durante el período de evaluación de 60 días, se puede realizar la conversión de un modo con licencia a un modo de evaluación. El tiempo disponible en el modo de evaluación se resta del tiempo ya consumido.

Por ejemplo, supongamos que se utiliza un host ESXi en el modo de evaluación durante 20 días y, a continuación, se asigna una clave de licencia de vSphere Standard Edition al host. Si se vuelve a establecer el host en el modo de evaluación, se podrá explorar el conjunto completo de funciones para el host durante el período de evaluación restante de 40 días.

Cuando expira el período de evaluación o la licencia de los hosts ESXi, estos se desconectan de vCenter Server. Todas las máquinas virtuales que estén encendidas continúan funcionando, pero no puede encender las máquinas virtuales una vez que se apagan. No puede cambiar la configuración actual de las características que están en uso. No se pueden utilizar las características que permanecieron sin usar antes de la caducidad de la licencia.

Para obtener información sobre la administración de licencias para los hosts ESXi, consulte la documentación *Administrar vCenter Server y hosts*.

Qué es VMware vSphere Distributed Services Engine® 3

vSphere Distributed Services Engine® es una capacidad de vSphere básica que permite a los clientes utilizar varias DPU con vSphere y VMware Cloud Foundation.

vSphere 8.0 permite un rendimiento de las cargas de trabajo sin precedentes para satisfacer las necesidades de rendimiento y latencia cada vez mayores. Con vSphere Distributed Services Engine, los servicios de infraestructura se distribuyen entre los diferentes recursos informáticos disponibles en el host ESXi, liberando a la DPU de algunas funciones de red. Esta capacidad funciona bien con las aplicaciones modernas, que se desarrollan utilizando un enfoque de arquitectura de microservicios que busca descomponer la aplicación en varios servicios independientes pero que colaboran. Esta mayor complejidad genera nuevas demandas para la CPU. Por ejemplo, procesar solicitudes de almacenamiento o transferir tráfico de red para estos microservicios deja menos ciclos de CPU para la carga de trabajo real. En este contexto, los aceleradores especialmente diseñados como las DPU pueden asumir la nueva carga informática y ayudar a mejorar el rendimiento y la eficiencia de la infraestructura.

Con vSphere Distributed Services Engine, las DPU pueden acelerar el rendimiento de la red y aumentar el rendimiento de los datos, a la vez que no suponen una carga operativa para la administración del ciclo de vida de las DPU, ya que la experiencia existente de Día 0, Día 1 y Día 2 de vSphere no cambia. vSphere Distributed Services Engine es compatible con unidades DPU de NVIDIA y AMD, y con diseños de servidor de Dell, HPE, Lenovo y Fujitsu. vSphere Distributed Services Engine está disponible en servidores con unidades DPU preinstaladas.

A partir de vSphere 8.0, puede descargar la funcionalidad que se ejecuta en la CPU principal en la DPU para mejorar significativamente el rendimiento de red y seguridad. Como se ilustra en el diagrama de arquitectura del vSphere continua, las DPU también pueden gestionar capacidades adicionales, como la descarga de almacenamiento y la administración nativa, pero actualmente no se admiten estas capacidades adicionales.

Figura 3-1. Arquitectura de vSphere continua.

OS APP
Storage: vSAN Data
Network and Security: NSX Svcs
Host Management
Compute Hypervisor
ESXi
Performance NIC
additional capabilities, currently not supported
Compute Hypervisor
Bare Metal Windows & Linux
ESXi
Security Airgap
DPU
Network and Security: NSX Services
Storage: vSAN Data
Host Management
ESXi

vSphere Distributed Services Engine descarga y acelera las funciones de infraestructura en la DPU mediante la introducción de un VMware vSphere Distributed Switch en la DPU y NSX Networking and Observability de VMware, que permite supervisar, identificar y mitigar de forma proactiva los cuellos de botella de la infraestructura de red sin derivaciones a la red complejas. La DPU se convierte en un nuevo punto de control para escalar funciones de infraestructura y habilita controles de seguridad sin agente y desacoplados del dominio de la carga de trabajo.

Con vSphere Distributed Services Engine podrá:

- Instalar y actualizar imágenes ESXi simultáneamente en el servidor x86 y la DPU compatible asociada para reducir la sobrecarga operativa de la administración del ciclo de vida de las unidades DPU con flujos de trabajo de vSphere integrados. Para obtener más información, consulte Usar vSphere Lifecycle Manager con VMware vSphere Distributed Services Engine.
- Establecer alarmas para alertas de hardware de DPU y supervisar las métricas de rendimiento del núcleo, la memoria y la red desde interfaces conocidas de vCenter, sin necesidad de nuevas herramientas. Para obtener más información, consulte CPU (DPU) y Memoria (DPU).
- Acelerar vSphere Distributed Switch en la DPU para mejorar el rendimiento de la red y utilizar ciclos de CPU disponibles para lograr una mayor consolidación de la carga de trabajo por host ESXi. Para obtener más información, consulte ¿Qué es la capacidad de descongestión de la red? y Crear una instancia de vSphere Distributed Switch.
- Conseguir compatibilidad con vSphere DRS y vSphere vMotion para máquinas virtuales que se ejecutan en hosts con DPU asociadas para obtener los beneficios del acceso directo sin sacrificar la portabilidad de la máquina virtual. Para obtener más información, consulte Clústeres homogéneos para DPU.

- Mejorar la seguridad de la infraestructura con seguridad de confianza cero. Para obtener más información, consulte Prácticas recomendadas de seguridad para vSphere Distributed Services Engine.

vSphere Distributed Services Engine no requiere una licencia de ESXi independiente. Una red interna que está aislada de otras redes conecta las DPU con los hosts ESXi. Las compilaciones del servidor ESXi 8.0 son imágenes unificadas, que contienen contenido x86 y DPU. En el sistema vSphere, las DPU se ven como objetos nuevos durante la instalación y la actualización, así como en los flujos de trabajo de perfiles de host, almacenamiento y redes.

Lea los siguientes temas a continuación:

Alta disponibilidad con VMware vSphere Distributed Services Engine

Con ESXi 8.0 Update 3, puede optar por una instalación de VMware vSphere Distributed Services Engine con dos unidades de procesamiento de datos (data processing unit, DPU) para lograr una alta disponibilidad.

En sistemas de vSphere con una sola DPU, el dispositivo puede convertirse en el único punto de error para las cargas de trabajo descargadas en la DPU, como las funciones de red, y que esto repercuta en los datos y la productividad. Con ESXi 8.0 Update 3, vSphere Distributed Services Engine también está disponible en servidores con dos DPU preinstaladas, lo que proporciona redundancia y resistencia de hardware.

Puede utilizar las dos DPU en modo activo/en espera para proporcionar alta disponibilidad. Esta configuración proporciona redundancia en el caso de que se produzca un error en una de las DPU. En la configuración de alta disponibilidad, ambas DPU se asignan a la misma instancia de vSphere Distributed Switch respaldada por NSX. Por ejemplo, DPU-1 se asocia a vmnic0 y vmnic1 de vSphere Distributed Switch y DPU-2 se asocia a vmnic2 y vmnic3 de la misma instancia de vSphere Distributed Switch.

También puede utilizar las dos DPU como dispositivos independientes para aumentar la capacidad de descarga por host ESXi. Cada DPU se asocia a una instancia de vSphere Distributed Switch independiente y no hay conmutación por error entre las DPU en dicha configuración.

Los sistemas de doble DPU pueden utilizar dispositivos NVIDIA o Pensando. En ESXi 8.0 Update 3, los sistemas de doble DPU son compatibles con los diseños de servidor de Lenovo. Los dispositivos de DPU que están en un servidor de doble DPU deben ser idénticos en todos los aspectos: el mismo proveedor, la misma versión de hardware y el mismo firmware. Para obtener una lista de los proveedores actuales y los diseños de servidor para VMware vSphere Distributed Services Engine, consulte la Guía de compatibilidad de VMware.

Instalación de VMware vSphere Distributed Services Engine con dos DPU

vSphere Distributed Services Engine no requiere una licencia de ESXi independiente. Las compilaciones de servidor de ESXi 8.0 Update 3 son imágenes unificadas, las cuales contienen contenido de x86 y DPU, y no se puede instalar contenido de x86 y DPU por separado.
El procedimiento de instalación en ambas DPU, ya sean interactivas o generadas por script, también se produce en paralelo y se observa una pérdida de rendimiento mínima en comparación con un sistema de una DPU.

Con vSphere 8.0 Update 3, puede obtener una configuración de servidor preinstalada con dos DPU de Dell o Lenovo, o bien puede agregar una segunda DPU a un sistema de una DPU en los servidores de doble DPU compatibles de Dell o Lenovo.

Nota En cualquier caso, debe ejecutar una nueva instalación completa de ESXi 8.0 Update 3 en el sistema, no solo en las DPU recién agregadas.

Para obtener más información sobre la instalación, consulte Instalar ESXi de forma interactiva y Scripts de instalación y actualización utilizados para la instalación de ESXi.

Gestión de errores, conmutación por error y reversión para VMware vSphere Distributed Services Engine

Antes de instalar VMware vSphere Distributed Services Engine, consulte las opciones de gestión de errores, conmutación por error y reversión.

Gestión de errores

Un error en la instalación del contenido x86 y DPU en un host ESXi marca todo el procedimiento de instalación como erróneo.

Si bien lo que se espera es que el estado del software de las DPU siga siendo idéntico en todo momento, en el poco probable caso de que se produzca un error durante una operación de ciclo de vida, como la instalación o la actualización de un componente, la operación puede realizarse correctamente en una DPU, pero puede producirse un error en la otra. Dado que cada operación de ciclo de vida se produce dentro de los límites de cada DPU, los errores no afectan al estado de la otra DPU, pero el resultado general de la instalación sí sigue marcado como error.

Durante la instalación interactiva, en los flujos de trabajo de vSphere Lifecycle Manager, y cuando se utiliza ESXCLI, se recibe información sobre la DPU en la que se produjo un error en la operación.

Tras una instalación correcta, en caso de haber errores de DPU, la acción recomendada es reiniciar el host ESXi afectado. Si sigue siendo posible acceder a la DPU desde el host, la recopilación de paquetes de registro general es suficiente para la solución de problemas. Si no se puede acceder a la DPU desde el host, el inicio de sesión en la DPU desde una interfaz BMC, iLO o iDRAC puede proporcionar registros de solución de problemas.

Conmutación por error

La compatibilidad con la conmutación por error en vSphere 8.0 Update 3 se limita a que una de las DPU deje de funcionar debido a errores de software dentro de la DPU o a una desconexión física de una de las DPU, como la desconexión de cable. No se admite la conmutación por error debido a errores de nivel de interconexión de componentes periféricos (Peripheral Component Interconnect, PCI).

Revertir

La reversión es un mecanismo de mejor esfuerzo para restaurar el sistema a un estado de funcionamiento anterior en caso de que se produzca un error antes de la fase de inicio del arranque de ESXi. La reversión en ambos servidores x86 y las DPU compatibles asociadas es automática en caso de que se produzca un error durante el arranque. También puede optar por una reversión manual si pulsa **`Mayús+R`** antes de que se inicie el cargador de arranque para volver a un buen estado anterior.

Cualquier error que se produzca después de que se inicie la fase de inicio no provoca una reversión.

Tabla 3-1. Escenarios de reversión para la instalación de VMware vSphere Distributed Services Engine

Situación	Número de reinicios necesarios
Ambas DPU arrancan correctamente. ESXi no arranca correctamente.	2
Ambas DPU no arrancan correctamente. ESXi arranca correctamente.	1
Una de las DPU arranca con una versión anterior a la otra DPU y ESXi.	2
Una de las DPU arranca con una versión anterior a la otra DPU y ESXi no arranca correctamente.	2

Instalar y configurar ESXi

4

Se puede instalar y configurar ESXi en el hardware físico de modo que actúe como plataforma para las máquinas virtuales.

Lea los siguientes temas a continuación:

Requisitos de ESXi

Para instalar o actualizar ESXi, el sistema debe cumplir con requisitos de hardware y software específicos.

Descripción general del almacenamiento del sistema ESXi

ESXi 8.0 tiene un diseño de almacenamiento del sistema que permite la administración flexible de particiones y componentes de terceros, a la vez que facilita la depuración.

Almacenamiento del sistema ESXi

El diseño del almacenamiento del sistema ESXi 8.0 consta de cuatro particiones:

Tabla 4-1. particiones de almacenamiento del sistema ESXi:

Partición	Uso	Tipo
Arranque del sistema	Almacena el cargador de arranque y los módulos EFI.	FAT16
Boot-bank 0	Espacio del sistema destinado a almacenar los módulos de arranque de ESXi.	FAT16

Tabla 4-1. particiones de almacenamiento del sistema ESXi: (continuación)

Partición	Uso	Tipo
Boot-bank 1	Espacio del sistema destinado a almacenar los módulos de arranque de ESXi.	FAT16
ESX-OSData	Actúa como la ubicación unificada para almacenar módulos adicionales. No se utiliza para los arranques ni las máquinas virtuales. Consolida la partición `/scratch` heredada, la partición del bloqueador para VMware Tools y los destinos de volcado de núcleo. **Precaución** En caso de que el medio de instalación sea un dispositivo de tarjeta SD o USB, la práctica recomendada es crear particiones ESX-OSData en un dispositivo de almacenamiento persistente que no se comparta entre hosts ESXi.	VMFS-L

El volumen ESX-OSData se divide en dos categorías de datos de alto nivel: datos persistentes y no persistentes. Los datos persistentes contienen datos que se escriben con poca frecuencia; por ejemplo, archivos ISO de VMware Tools, configuraciones y volcados de núcleo.

Los datos no persistentes contienen datos que se escriben con frecuencia; por ejemplo, registros, seguimientos globales de VMFS, datos del daemon de persistencia de entrada (Entry Persistence Daemon, EPD) de vSAN, seguimientos de vSAN y bases de datos en tiempo real.

Figura 4-1. Almacenamiento del sistema consolidado en ESXi 8.0

Diseño del almacenamiento
del sistema ESXi 6.x
4 MB arranque del sistema
250 MB boot-bank 0
250 MB boot-bank 1
110 MB volcado de núcleo pequeño
286 MB locker
(se crea si los medios >3,4 GB) 2,5 GB volcado de núcleo grande
4 GB scratch
(se crea si los medios >8,5 GB
no se crean en la unidad flash USB)
almacén de datos de VMFS

ESXi 7.0 y versiones posteriores
Diseño de almacenamiento del sistema para
arranque del sistema 100 MB
boot-bank 0 De 500 MB a 4 GB, (en función del tamaño del medio de arranque utilizado)
boot-bank 1 De 500 MB a 4 GB, (en función del tamaño del medio de arranque utilizado)
ESX-OS Data
Datos de ROM
Datos de RAM
espacio restante, hasta 128 GB
almacén de datos de VMFS espacio restante, (para el tamaño de medios >142 GB)

Tamaños del almacenamiento del sistema ESXi

A excepción de la partición de arranque del sistema, los tamaños de las particiones pueden variar en función del tamaño de los medios de arranque que se utilicen. Si el medio de arranque es de gran resistencia con una capacidad superior a 142 GB, se crea automáticamente un almacén de datos de VMFS para almacenar los datos de la máquina virtual.

Si desea revisar la capacidad de los medios de arranque y el ajuste de tamaño automático que configura el instalador de ESXi, utilice vSphere Client y vaya a la vista **Detalles de particiones**. Si lo prefiere, puede usar ESXCLI; por ejemplo, el comando `esxcli storage filesystem list`.

Tabla 4-2. Tamaños del almacenamiento del sistema ESXi en función del medio de arranque que se utilice y su capacidad

Tamaño del medio de arranque	8 a 10 GB	10 a 32 GB	32 a 128 GB	>128 GB
Arranque del sistema	100 MB	100 MB	100 MB	100 MB
Boot-bank 0	500 MB	1 GB	4 GB	4 GB
Boot-bank 1	500 MB	1 GB	4 GB	4 GB
ESX-OSData	espacio restante	espacio restante	espacio restante	hasta 128 GB
almacén de datos de VMFS				espacio restante para el tamaño de medios >142 GB

Se puede usar la opción de arranque del instalador de ESXi `systemMediaSize` para limitar el tamaño de las particiones de almacenamiento del sistema en el medio de arranque. Si el sistema tiene un espacio pequeño que no requiere el tamaño máximo de almacenamiento del sistema de 128 GB, puede limitarlo al mínimo de 32 GB. El parámetro `systemMediaSize` acepta los siguientes valores:

- min (32 GB, para servidores integrados o con un único disco)
- small (64 GB, para servidores con al menos 512 GB de RAM)
- default (128 GB)
- max (consumir todo el espacio disponible, para servidores de varios terabytes)

El valor seleccionado debe adecuarse al propósito del sistema. Por ejemplo, un sistema con 1 TB de memoria debe usar un mínimo de 64 GB para el almacenamiento del sistema. Para establecer la opción de arranque en el momento de la instalación (por ejemplo, `systemMediaSize=small`), consulte Introducir las opciones de arranque para iniciar un script de instalación o actualización. Para obtener más información, consulte el artículo 81166 de la base de conocimientos.

Vínculos del almacenamiento del sistema ESXi

Los subsistemas que requieren acceso a las particiones de ESXi acceden a estas particiones mediante los siguientes vínculos simbólicos:

Tabla 4-3. Vínculos simbólicos del almacenamiento del sistema ESXi

Volumen del almacenamiento del sistema	Vínculo simbólico
Boot-bank 0	`/bootbank`
Boot-bank 1	`/altbootbank`

Tabla 4-3. Vínculos simbólicos del almacenamiento del sistema ESXi (continuación)

Volumen del almacenamiento del sistema	Vínculo simbólico
Datos persistentes	/productLocker /locker /var/core /usr/lib/vmware/isoimages /usr/lib/vmware/floppies
Datos no persistentes	/var/run /var/log /var/vmware /var/tmp /scratch

Comportamiento de almacenamiento

Al iniciar ESXi, el host entra en una fase de autoconfiguración durante la que se configuran los dispositivos de almacenamiento del sistema con los valores predeterminados.

Cuando reinicie el host ESXi después de instalar la imagen de ESXi, el host configura los dispositivos de almacenamiento del sistema con la configuración predeterminada. A partir de ESXi 7.0, puede activar la opción `autoPartition`, la cual formatea automáticamente todos los dispositivos vacíos disponibles con VMFS, excepto los dispositivos SD y USB heredados. El valor predeterminado es `autoPartition=FALSE`, que formatea dispositivos de arranque solo con VMFS con un tamaño superior a 128 GB. Para obtener más información, consulte el artículo 77009 de la base de conocimientos de VMware.

Precaución ESXi sobrescribe cualquier disco que parezca estar vacío. Los discos se consideran vacíos si no poseen una tabla de particiones o particiones válidas. Si usa software que utiliza dichos discos, en particular si está utilizando un administrador de volúmenes lógicos (LVM) en lugar de o además de esquemas tradicionales de particionamiento, ESXi podría causar un reformateo del LVM local. Realice una copia de seguridad de los datos del sistema antes de habilitar ESXi por primera vez.

En el disco duro o dispositivo USB desde el que arranca el host ESXi, el software de formateo de discos conserva las particiones de diagnóstico existentes que el proveedor de hardware crea. En el espacio restante, el software crea las particiones descritas a continuación.

Particiones creadas por ESXi en la unidad del host

Para instalaciones nuevas, se crean varias particiones nuevas para el arranque del sistema, los bancos de arranque y ESX-OSData. La instalaciones desde cero de ESXi utilizan las tablas de particiones GUID (GPT) en lugar del particionamiento basado en MSDOS. El instalador crea bancos de arranque de diferentes tamaños en función del tamaño del disco. Para obtener más información sobre la partición desde cero, consulte Acerca de la partición desde cero.

El instalador afecta solamente al disco de instalación. El instalador no afecta a otros discos del servidor. Cuando se realiza la instalación en un disco, el instalador sobrescribe el disco completo. Cuando el instalador configura automáticamente el almacenamiento, no sobrescribe las particiones del proveedor de hardware.

Para crear el almacén de datos de VMFS, el instalador de ESXi necesita un mínimo de 128 GB de espacio disponible en el disco de instalación.

Es posible que desee anular este comportamiento predeterminado si, por ejemplo, utiliza dispositivos de almacenamiento compartido en lugar de almacenamiento local. A fin de evitar un formateo automático de discos, desconecte los dispositivos de almacenamiento local del host en las siguientes circunstancias:

- Antes de ejecutar el host por primera vez.
- Antes de ejecutar el host después de restablecerlo a los valores predeterminados de configuración.

Para anular el formateo VMFS, si ya se realizó el formateo automático de discos, puede eliminar el almacén de datos. Consulte la documentación de *Administrar vCenter Server y hosts*.

Acerca de la partición desde cero

En las instalaciones nuevas de ESXi, durante la fase de configuración automática, se crea una partición desde cero como parte de la partición ESX-OSDATA.

Nota La partición de hosts que se actualizan a ESXi 7.0 y versiones posteriores a partir de versiones anteriores varía de manera significativa respecto de la partición de las nuevas instalaciones de ESXi. El proceso de actualización a ESXi 7.0 y otras versiones posteriores vuelve a particionar el dispositivo de arranque y consolida el volcado de núcleo, el bloqueador y las particiones desde cero originales en el volumen ESX-OSData.

La partición desde cero se usa para almacenar registros del sistema que se necesitan cuando se crea un paquete de soporte. Si no hay ninguna partición desde cero, los registros del sistema se almacenan en un disco RAM. Si no se crea ninguna partición desde cero, puede configurar una. También puede anular la configuración predeterminada.

La partición desde cero se puede crear en un directorio remoto montado en SAN o NFS.

Establecer la partición desde cero de vSphere Client

Si no hay configurada ninguna partición desde cero, es posible que quiera configurar una, especialmente si el host tiene poca memoria. Cuando no hay ninguna partición desde cero, los registros del sistema se almacenan en un disco RAM.

Requisitos previos

El directorio que se usará para la partición temporal debe existir en el host.

Procedimiento

1 Desde vSphere Client, conéctese a vCenter Server.

2 Seleccione el host en el inventario.

3 Haga clic en la pestaña **Configurar**.

4 Seleccione **Sistema**.

5 Seleccione **Configuración avanzada del sistema**.

   El parámetro **ScratchConfig.CurrentScratchLocation** muestra la ubicación actual de la partición desde cero.

6 En el cuadro de texto **ScratchConfig.ConfiguredScratchLocation**, introduzca una ruta de acceso de directorio que sea exclusiva para este host.

   Por ejemplo, **`/vmfs/volumes/`*`DatastoreUUID`*`/`*`DatastoreFolder`***.

7 Reinicie el host para que se apliquen los cambios.

Requisitos de hardware de ESXi

Asegúrese de que el host cumpla la configuración de hardware mínima de ESXi8.0.

Recursos de hardware y del sistema

Para instalar o actualizar ESXi, los recursos de hardware y del sistema deben cumplir los siguientes requisitos:

- Plataforma de servidores compatible. Para obtener una lista de plataformas compatibles, consulte la *Guía de compatibilidad de VMware* en http://www.vmware.com/resources/compatibility.
- ESXi 8.0 requiere un host con al menos dos núcleos de CPU.
- ESXi 8.0 admite una amplia gama de procesadores x86 de 64 bits de varios núcleos. Para obtener una lista completa de procesadores compatibles, consulte la guía de compatibilidad de VMware en http://www.vmware.com/resources/compatibility.
- ESXi 8.0 requiere que el bit NX/XD esté habilitado para la CPU en el BIOS.
- ESXi 8.0 requiere un mínimo de 8 GB de RAM física. Proporcione al menos 12 GB de RAM para ejecutar máquinas virtuales en entornos de producción típicos.
- Para admitir máquinas virtuales de 64 bits, se debe habilitar la compatibilidad para virtualización de (Intel VT-x o RVI AMD) en CPU x64.
- Una o más controladoras Gigabit o Ethernet más rápidas. Para obtener una lista de modelos de adaptadores de red compatibles, consulte la *Guía de compatibilidad de VMware* en http://www.vmware.com/resources/compatibility.
- ESXi 8.0 requiere un disco de arranque de al menos 32 GB de almacenamiento persistente, como HDD, SSD o NVMe. No se debe compartir un dispositivo de arranque entre hosts ESXi.
- Disco SCSI o un LUN RAID local que no sea de red con espacio sin particionar para las máquinas virtuales.

- Para la serie ATA (SATA), un disco conectado a través de controladoras SAS compatibles o controladoras SATA integradas compatibles. Los discos SATA se consideran remotos, no locales. Estos discos no se usan como una partición desde cero de forma predeterminada, ya que se consideran remotos.

  Nota No puede conectar un dispositivo CD-ROM SATA a una máquina virtual en un host ESXi. Para usar el dispositivo CD-ROM SATA, debe usar el modo de emulación IDE.

Sistemas de almacenamiento

Para obtener una lista de sistemas de almacenamiento compatibles, consulte la *Guía de compatibilidad de VMware* en http://www.vmware.com/resources/compatibility. A partir de ESXi 8.0, no se pueden utilizar adaptadores de software para canal de fibra en Ethernet (Fibre Channel over Ethernet, FCoE), solo adaptadores de FCoE de hardware.

Requisitos de arranque de ESXi

En vSphere 8.0, la compatibilidad con BIOS heredado es limitada y se recomienda arrancar los hosts ESXi desde la Unified Extensible Firmware Interface (UEFI). Con la UEFI, puede arrancar sistemas desde unidades de disco duro, unidades de CD-ROM o medios USB. vSphere Auto Deploy admite el arranque de redes y el aprovisionamiento de hosts ESXi mediante UEFI. Si el sistema tiene unidades de procesamiento de datos (DPU) admitidas, solo puede usar UEFI para instalar y arrancar ESXi en las DPU. Para obtener más información sobre los planes de VMware para dejar de admitir BIOS heredado en plataformas de servidor, consulte el artículo https://kb.vmware.com/s/article/84233 de la base de conocimientos.

ESXi puede arrancar desde un disco con más de 2 TB siempre que el firmware del sistema y el firmware en cualquier tarjeta adicional que esté usando lo admitan. Consulte la documentación del proveedor.

Requisitos de almacenamiento para la instalación o actualización de ESXi 8.0

Para obtener el mejor rendimiento de una instalación de ESXi 8.0 utilice un dispositivo de almacenamiento persistente con un mínimo de 32 GB para los dispositivos de arranque. La actualización a ESXi 8.0 requiere un dispositivo de arranque de al menos 8 GB. Al arrancar desde un disco local, un LUN iSCSI o SAN, se necesita un disco de al menos 32 GB para permitir la creación de volúmenes de almacenamiento del sistema, incluida una partición de arranque, bancos de arranque y un volumen ESX-OSData basado en VMFS-L. El volumen ESX-OSData asume la función de la partición heredada `/scratch`, la partición de bloqueador para VMware Tools y el destino del volcado de núcleo.

Nota En ESXi 8.0, el volumen ESX-OSData se considera una partición unificada y los componentes independientes, como `/scratch` y VMware Tools, están consolidados en una sola partición persistente de OSDATA.

Otras opciones para obtener el mejor rendimiento de una instalación de ESXi 8.0 son las siguientes:

- Un disco local de 128 GB o más para ofrecer una compatibilidad óptima con ESX-OSData. El disco contiene la partición de arranque, el volumen ESX-OSData y un almacén de datos de VMFS.
- Un dispositivo que admite un mínimo de 128 Terabytes escritos (terabytes written, TBW).
- Un dispositivo que proporciona al menos 100 MB/s de velocidad de escritura secuencial.
- Para proporcionar resiliencia en caso de que se produzca un error en el dispositivo, se recomienda un dispositivo reflejado RAID 1.

Con las siguientes limitaciones, se admiten los dispositivos USB y SD heredados:

- Los dispositivos SD y USB se admite para las particiones de banco de arranque. El uso de dispositivos SD y USB para almacenar particiones ESX-OSData está obsoleto y la práctica recomendada consiste en proporcionar un dispositivo local persistente independiente con un mínimo de 32 GB para almacenar el volumen ESX-OSData. El dispositivo de arranque local persistente puede ser un dispositivo flash M.2 de grado industrial (SLC y MLC), SAS, SATA, HDD, SSD o NVMe. La capacidad óptima para los dispositivos locales persistentes es de 128 GB.
- Si no proporciona almacenamiento persistente, verá una alarma del tipo `No se encontró ningún dispositivo persistente secundario. Mueva la instalación a almacenamiento persistente, ya que la compatibilidad con la configuración solo de tarjeta SD/USB va a dejar de utilizarse`.
- Debe utilizar un dispositivo flash SD aprobado por el proveedor del servidor para el modelo de servidor en particular en el que desea instalar ESXi en un dispositivo de almacenamiento flash SD. Puede encontrar una lista de dispositivos validados en partnerweb.vmware.com.
- Consulte el artículo de la base de conocimientos 85685 sobre las instrucciones actualizadas para entornos basados en tarjetas SD o USB.
- Para elegir un dispositivo de arranque SD o USB adecuado, consulte el artículo 82515 de la base de conocimientos.

El proceso de actualización a ESXi 8.0 desde versiones anteriores a la 7.x vuelve a particionar el dispositivo de arranque y consolida el volcado de núcleo, el bloqueador y las particiones scratch originales en el volumen ESX-OSData.

Los siguientes eventos se producen durante el proceso de reparticionamiento:

- Si no se configura un destino de volcado de núcleo personalizado, la ubicación predeterminada es un archivo en el volumen ESX-OSData.
- Si el servicio de syslog está configurado para almacenar archivos de registro en la partición temporal de VFAT de 4 GB, los archivos de registro de `var/run/log` se migran al volumen ESX-OSData.
- VMware Tools se migra de la partición del bloqueador y se borra la partición.

- Se elimina la partición de volcado de núcleo. Se eliminan los archivos de volcado de núcleo de la aplicación que se almacenan en la partición temporal.

Nota No es posible revertir de ESXi 8.x a una versión de ESXi anterior a la versión 7.x debido al proceso de nueva partición del dispositivo de arranque. Para utilizar una versión de ESXi anterior a la versión 7.x después de actualizar a la versión 8.0, debe crear una copia de seguridad del dispositivo de arranque antes de la actualización y restaurar el dispositivo de arranque de ESXi a partir de la copia de seguridad. La reversión de ESXi 8.x a 7.x es posible siempre que no se hayan realizado cambios en las particiones bootbank y no se detecte ninguna partición dañada.

Si utiliza dispositivos USB o SD para realizar una actualización, la práctica recomendada es asignar una región ESX-OSData en un disco persistente disponible o un LUN de SAN. Si no hay disponibles almacenamiento persistente o un LUN de SAN, ESX-OSData se crea automáticamente en un disco RAM. VMFS también se puede utilizar para la partición ESX-OSData.

Después de la actualización, si ESX-OSData reside en un disco RAM, un nuevo dispositivo persistente se encuentra en arranques posteriores y ese dispositivo tiene el ajuste `autoPartition=True`, ESX-OSData se crea automáticamente en el nuevo dispositivo persistente. ESX-OSData no se mueve automáticamente entre almacenamientos persistentes, pero es posible cambiar manualmente la ubicación de ESX-OSData a un almacenamiento compatible.

Para volver a configurar `/ scratch`, consulte Establecer la partición temporal desde vSphere Client.

Para configurar el tamaño de las particiones del sistema ESXi, puede utilizar la opción `systemMediaSize`. Para obtener más información, consulte el artículo https://kb.vmware.com/s/article/81166 de la base de conocimientos.

En instalaciones de Auto Deploy, el instalador intenta asignar una región temporal en un disco o un almacén de datos local disponible. Si no se encuentra ningún disco o almacén de datos local, se producirá un error en la instalación.

En los entornos que arrancan desde una SAN o utilizan Auto Deploy, el volumen ESX-OSData para cada host ESXi debe configurarse en un LUN de SAN separado.

Usar aplicaciones de administración remota

Las aplicaciones de administración remota permiten instalar ESXi en servidores que se encuentran en ubicaciones remotas.

Las aplicaciones de administración remota compatibles para la instalación incluyen HP Integrated Lights-Out (iLO), Dell Remote Access Card (DRAC), IBM management module (MM), Fujitsu iRMC y Remote Supervisor Adapter II (RSA II). Para obtener soporte técnico para las aplicaciones de administración remota, póngase en contacto con el proveedor.

Puede usar aplicaciones de administración remota para realizar instalaciones interactivas y por script de ESXi de forma remota.

Si utiliza aplicaciones de administración remota para instalar ESXi, el CD virtual podría encontrarse con daños en sistemas o redes que operan a capacidad máxima. Si se produce un error en una instalación remota de una imagen ISO, complete la instalación desde el CD físico.

Modelos de servidores de administración remota compatibles y versiones de firmware

Puede utilizar aplicaciones de administración remota para instalar o actualizar ESXi o para administrar hosts de forma remota.

Tabla 4-4. Modelos de servidores de administración remota compatibles y versiones de firmware mínimas

Modelo de servidor de administración remota	Versión de firmware	Java
Dell DRAC 9	6.0.30.00	N/C
Dell DRAC 7	1.30.30 (compilación 43)	1.7.0_60-b19
Dell DRAC 6	1.54 (compilación 15), 1.70 (compilación 21)	1.6.0_24
Dell DRAC 5	1.0, 1.45, 1.51	1.6.0_20,1.6.0_203
Dell DRAC 4	1.75	1.6.0_23
Fujitsu iRMC S5	1.10P	1.7.0_60-b19
Fujitsu iRMC S6	1.06S	N/C
ILO HP	1.81, 1.92	1.6.0_22, 1.6.0_23
ILO HP 2	1.8, 1.81	1.6.0_20, 1.6.0_23
ILO HP 3	1.28	1.7.0_60-b19
ILO HP 4	1.13	1.7.0_60-b19
ILO HP 5	2.72	N/C
RSA IBM 2	1.03, 1.2	1.6.0_22

Recomendaciones para un rendimiento mejorado de ESXi

Para mejorar el rendimiento, instale o actualice ESXi en un sistema robusto con más RAM que el mínimo necesario y con varios discos físicos.

Para conocer los requisitos del sistema de ESXi, consulte Requisitos de hardware de ESXi.

Tabla 4-5. Recomendaciones para un mejor rendimiento

Elemento del sistema	Recomendación
RAM	Los hosts ESXi requieren más RAM que los servidores típicos. ESXi 8.0 requiere un mínimo de 8 GB de RAM física. Proporcione al menos 12 GB de RAM para aprovechar al máximo las características de ESXi y ejecutar máquinas virtuales en entornos de producción típicos. Un host ESXi debe tener suficiente RAM para que funcionen máquinas virtuales simultáneas. Se proporcionan los siguientes ejemplos para ayudar a calcular la RAM que necesitan las máquinas virtuales que se ejecutan en el host ESXi. Para operar cuatro máquinas virtuales con Red Hat Enterprise Linux o Windows XP se requiere al menos 3 GB de RAM para rendimiento línea base. Esta cifra incluye 1.024 MB para las máquinas virtuales, 256 MB como mínimo para cada sistema operativo, según lo que recomiendan los proveedores. Para que estas cuatro máquinas virtuales funcionen con 512 MB de RAM, es necesario que los hosts ESXi tengan 4 GB de RAM, lo que incluye 2.048 MB para las máquinas virtuales. Estos cálculos no incluyen los posibles ahorros de memoria derivados de usar memoria con sobrecarga variable para cada máquina virtual. Consulte *Administración de recursos de vSphere*.
Adaptadores Fast Ethernet dedicados para máquinas virtuales	Coloque la red de administración y las redes de máquinas virtuales en tarjetas de red físicas distintas. Las tarjetas Gigabit Ethernet dedicadas para máquinas virtuales, como adaptadores Intel PRO 1000, mejoran el rendimiento para máquinas virtuales con gran tráfico de red.
Ubicación del disco	Coloque todos los datos que usan las máquinas virtuales en discos físicos asignados específicamente a máquinas virtuales. El rendimiento es mejor cuando no coloca las máquinas virtuales en el disco que contiene la imagen de arranque de ESXi. Use discos físicos que sean lo bastante grandes para mantener imágenes del disco que usan todas las máquinas virtuales.
Partición de VMFS6	El instalador de ESXi crea los volúmenes iniciales de VMFS en el primer disco local en blanco que se encuentra. Para agregar discos o modificar la configuración original, use vSphere Client. Esta práctica asegura que los sectores de arranque de las particiones estén alineados con 64K, lo que mejora el rendimiento del almacenamiento. **Nota** Para entornos únicamente de SAS, es posible que el instalador no formatee los discos. Para algunos discos SAS, no es posible identificar si los discos son locales o remotos. Después de la instalación, se puede usar vSphere Client para configurar VMFS.

Tabla 4-5. Recomendaciones para un mejor rendimiento (continuación)

Elemento del sistema	Recomendación
Procesadores	Los procesadores más rápidos mejoran el rendimiento de ESXi. Para ciertas cargas de trabajo, una mayor cantidad de memorias caché mejoran el rendimiento de ESXi.
Compatibilidad de hardware	Use dispositivos en el servidor que sean compatibles con controladores de ESXi. Consulte la *Guía de compatibilidad de hardware* en http://www.vmware.com/resources/compatibility.

Puertos de firewall entrantes y salientes para hosts de ESXi

Abra y cierre los puertos de firewall de cada servicio mediante vSphere Client o VMware Host Client.

ESXi incluye un firewall que está habilitado de forma predeterminada. En el momento de realizar la instalación, el firewall de ESXi se configura para bloquear el tráfico entrante y saliente, excepto el tráfico de los servicios que están habilitados en el perfil de seguridad del host. Para obtener la lista de los puertos y protocolos compatibles en el firewall de ESXi, consulte la herramienta VMware Ports and Protocols™ en https://ports.vmware.com/.

La herramienta VMware Ports and Protocols muestra la información sobre los puertos de los servicios que se instalan de forma predeterminada. Si instala otros VIB en el host, es posible que estén disponibles otros puertos de firewall y servicios adicionales. La información es principalmente para los servicios que están visibles en vSphere Client, pero la herramienta VMware Ports and Protocols también incluye otros puertos.

Espacio libre necesario para registro del sistema

Consulte la configuración recomendada de tamaño y rotación mínima para registros hostd, vpxa y fdm.

Si utilizó Auto Deploy para instalar el host ESXi 8.0 o bien si configuró un directorio de registro separado de la ubicación predeterminada en un directorio totalmente nuevo en el volumen de VMFS, es posible que deba cambiar su configuración de tamaño y rotación de registro actual para garantizar que el espacio disponible sea suficiente para el registro del sistema. Todos los componentes de vSphere usan esta infraestructura. Los valores predeterminados para la capacidad de registros en esta infraestructura varían según la cantidad de almacenamiento disponible y cómo ha configurado el registro del sistema. Los hosts que se implementan con Auto Deploy almacenan registros en un disco RAM, lo que significa que hay poca cantidad de espacio disponible para registros.

Si su host se implementa con Auto Deploy, vuelva a configurar el almacenamiento de sus registros de una de estas formas:

- Redirija los registros a través de la red hacia un recopilador remoto.
- Redirija registros hacia un almacenamiento NAS o NFS.

Si redirige los registros hacia un almacenamiento no predeterminado, como NAS o NFS, es posible que también desee volver a configurar el dimensionamiento y las rotaciones de los registros para los hosts que están instalados en el disco.

No tiene que volver a configurar el almacenamiento de registros para hosts ESXi que utilizan la configuración predeterminada, que almacena registros en un directorio temporal en el volumen de VMFS. Para estos hosts, ESXi 8.0 configura registros que se adapten de la mejor manera a cada instalación y proporciona suficiente espacio para alojar mensajes de registros.

Tabla 4-6. Configuración recomendada de tamaño y rotación mínima para registros hostd, vpxa y fdm

Registro	Tamaño máximo de archivo de registro	Número de archivos de registro que se van a conservar	Espacio de disco mínimo necesario
Agente de administración (hostd)	10 MB	10	100 MB
Agente VirtualCenter (vpxa)	5 MB	10	50 MB
Agente de vSphere HA (administrador de dominio de fallas, fdm)	5 MB	10	50 MB

Para obtener información sobre la configuración de un servidor de registro remoto, consulte Configurar Syslog en hosts ESXi.

De manera opcional, puede instalar VMware vCenter Log Insight, que brinda agregado y análisis de registros.

Requisitos del sistema de VMware Host Client

Asegúrese de que su explorador sea compatible con VMware Host Client.

Los siguientes sistemas operativos invitados y las siguientes versiones de exploradores web son compatibles con VMware Host Client.

Exploradores compatibles	Mac OS	Windows de 32 bits y 64 bits	Linux
Google Chrome	89+	89+	75+
Mozilla Firefox	80+	80+	60+
Microsoft Edge	90+	90+	N/C
Safari	9.0+	N/C	N/C

Bloqueo de cuenta y contraseñas ESXi

Para los hosts ESXi, debe utilizar una contraseña con requisitos predefinidos. Puede cambiar el requisito de longitud requerida y la clase de caracteres o permitir frases de contraseña si utiliza

el ajuste del sistema avanzado `Security.PasswordQualityControl`. También puede establecer el número de contraseñas para recordar para cada usuario mediante el ajuste del sistema avanzado `Security.PasswordHistory`.

Nota Los requisitos predeterminados para las contraseñas de ESXi pueden cambiar de una versión a otra. Puede comprobar las restricciones predeterminadas para la contraseña y modificarlas con el ajuste del sistema avanzado `Security.PasswordQualityControl`.

Contraseñas de ESXi

ESXi aplica requisitos de contraseña para el acceso desde la interfaz de usuario de la consola directa, ESXi Shell, SSH o VMware Host Client.

- De manera predeterminada, debe incluir una combinación de al menos tres de las cuatro clases de caracteres siguientes: letras en minúscula, letras en mayúscula, números y caracteres especiales, como el guion bajo o el guion, al crear una contraseña.
- De forma predeterminada, la longitud de la contraseña debe tener como mínimo 7 caracteres y menos de 40.
- Las contraseñas no deben contener una palabra de diccionario ni parte de una palabra de diccionario.
- Las contraseñas no deben contener el nombre de usuario ni partes del mismo.

Nota Un carácter en mayúscula al inicio de una contraseña no se tiene en cuenta en la cantidad de clases de caracteres que se utilizan. Un número al final de una contraseña no se tiene en cuenta en la cantidad de clases de caracteres que se utilizan. Una palabra del diccionario que se utiliza dentro de una contraseña reduce la longitud general de la contraseña.

Ejemplos de contraseñas de ESXi

A continuación se indican posibles contraseñas en caso de configurar la opción de la siguiente manera.

```
retry=3 min=disabled,disabled,disabled,7,7
```

Con esta opción, se solicita al usuario hasta tres veces (retry=3) una contraseña nueva si no es lo suficientemente segura o si la contraseña no se introdujo correctamente dos veces. No se permiten las contraseñas que tienen una o dos clases de caracteres ni las frases de contraseña, ya que los primeros tres elementos están desactivados. Las contraseñas de tres y cuatro clases de caracteres requieren siete caracteres. Consulte la página del manual de `pam_passwdqc` para obtener más información sobre otras opciones, como `max` y `passphrase`, entre otras.

Con esta configuración, se permiten las siguientes contraseñas.

- xQaTEhb!: contiene ocho caracteres de tres clases.
- xQaT3#A: contiene siete caracteres de cuatro clases.

Las siguientes contraseñas posibles no cumplen con los requisitos.

- Xqat3hi: comienza con un carácter en mayúscula, lo que reduce la cantidad efectiva de clases de caracteres a dos. La cantidad mínima de clases de caracteres requerida es tres.
- xQaTEh2: termina con un número, lo que reduce la cantidad efectiva de clases de caracteres a dos. La cantidad mínima de clases de caracteres requerida es tres.

Frase de contraseña de ESXi

En lugar de una contraseña, también puede utilizar una frase de contraseña. Sin embargo, las frases de contraseña están desactivadas de forma predeterminada. Puede cambiar este valor predeterminado u otros valores de configuración mediante el ajuste del sistema avanzado `Security.PasswordQualityControl` de vSphere Client.

Por ejemplo, puede cambiar la opción por la siguiente.

```
retry=3 min=disabled,disabled,16,7,7
```

Este ejemplo permite frases de contraseña de al menos 16 caracteres y al menos tres palabras.

Modificar las restricciones predeterminadas de contraseña

Puede cambiar la restricción predeterminada de contraseñas y frases de contraseña con el ajuste del sistema avanzado `Security.PasswordQualityControl` para su host ESXi. Consulte la documentación de *Administrar vCenter Server y hosts* para obtener información sobre cómo cambiar los ajustes avanzados del sistema de ESXi.

Puede cambiar el valor predeterminado, por ejemplo, para requerir un mínimo de 15 caracteres y una cantidad mínima de cuatro palabras (`passphrase=4`) de la siguiente manera:

```
retry=3 min=disabled,disabled,15,7,7 passphrase=4
```

Para obtener más información, consulte la página del manual de `pam_passwdqc`.

Nota Aún no se han probado todas las combinaciones posibles de opciones de contraseña. Después de cambiar la configuración de contraseña predeterminada, realice una prueba adicional.

En este ejemplo, se establece el requisito de complejidad de contraseña para requerir ocho caracteres de cuatro clases que aplican una diferencia significativa de contraseñas, un historial recordado de cinco contraseñas y una directiva de rotación de 90 días:

```
min=disabled,disabled,disabled,disabled,8 similar=deny
```

Comportamiento del bloqueo de cuentas de ESXi

Se admite el bloqueo de cuentas para el acceso a través de SSH y vSphere Web Services SDK. La interfaz de la consola directa (DCUI) y ESXi Shell no admiten el bloqueo de cuentas. De forma predeterminada, se permite un máximo de cinco intentos con errores antes de que la cuenta se bloquee. De forma predeterminada, la cuenta se desbloquea después de 15 minutos.

Configurar el comportamiento de inicio de sesión

Puede configurar el comportamiento de inicio de sesión del host ESXi con los siguientes ajustes del sistema avanzados:

- `Security.AccountLockFailures`. Cantidad máxima de intentos de inicio de sesión con errores antes de que la cuenta de un usuario se bloquee. Cero desactiva el bloqueo de cuentas.
- `Security.AccountUnlockTime`. Cantidad de segundos en los que el usuario queda bloqueado.
- `Security.PasswordHistory`. Número de contraseñas que se deben recordar para cada usuario. A partir de vSphere 8.0 Update 1, el valor predeterminado es cinco. Cero desactiva el historial de contraseñas.

Consulte la documentación de *Administrar vCenter Server y hosts* para obtener información sobre la configuración de las opciones avanzadas de ESXi.

Preparativos para la instalación de ESXi

Antes de instalar ESXi, determine la opción de instalación más adecuada para el entorno y prepare el proceso de instalación.

Descarga del instalador de ESXi

El software del instalador de ESXi se puede obtener desde un OEM o desde el portal de soporte de Broadcom.

Regístrese en el portal de soporte de Broadcom. Para obtener más información, consulte Registrar una cuenta en las comunidades y en el portal de soporte de Broadcom.

Para ver instrucciones de descarga de productos, consulte Descargar productos y software de Broadcom.

Para descargar archivos ZIP de paquetes sin conexión para actualizaciones y revisiones de ESXi, consulte Descargar archivos y soluciones PTF de Broadcom.

Para obtener más información, consulte Preguntas frecuentes de VMware al soporte de Broadcom.

Información obligatoria para instalar ESXi

La instalación interactiva le solicita la información necesaria del sistema, pero debe proporcionar esta información en el script de instalación.

En una instalación interactiva, el sistema le solicita la información del sistema necesaria. En una instalación generada por script, debe proporcionar esta información en el script de instalación. Para su uso en el futuro, anote los valores que utilice durante la instalación. Estas anotaciones son útiles si debe reinstalar ESXi y volver a introducir los valores que seleccionó inicialmente.

Tabla 4-7. Información obligatoria para instalar ESXi

Información	Obligatorio u opcional	Predeterminado	Comentarios
Distribución del teclado	Obligatorio	Inglés (EE. UU.)	
Identificador de VLAN	Opcional	Ninguna	Rango: de 0 a 4094
Dirección IP	Opcional	DHCP	Puede permitir que DHCP configure la red durante la instalación. Después de la instalación, puede cambiar la configuración de red.
Máscara de subred	Opcional	Se calcula en base a la dirección IP	
Puerta de enlace	Opcional	En función de la dirección IP y la máscara de subred configuradas	
DNS principal	Opcional	En función de la dirección IP y la máscara de subred configuradas	
DNS secundario	Opcional	Ninguna	
Nombre de host	Obligatorio para la configuración de IP estática	Ninguna	vSphere Client puede utilizar el nombre de host o la dirección IP para acceder al host ESXi.
Ubicación de instalación	Obligatorio	Ninguna	Debe tener al menos 5 GB si va a instalar los componentes en un único disco.
Migrar la configuración de ESXi existente. Conservar el almacén de datos de VMFS existente.	Obligatorio si va a instalar ESXi en una unidad con una instalación de ESXi existente.	Ninguna	Si ya existe una instalación de ESXi 5.x, el instalador de ESXi permite elegir entre conservar o sobrescribir el almacén de datos de VMFS durante la instalación
Contraseña raíz	Obligatorio	Ninguna	La contraseña raíz debe contener entre 8 y 40 caracteres. Para obtener información sobre las contraseñas, consulte la documentación sobre la *seguridad de vSphere*.

Opciones de medios para arrancar el instalador de ESXi

El instalador de ESXi debe ser accesible para el sistema en el que se va a instalar ESXi.

Los siguientes medios de arranque son compatibles con el instalador de ESXi:

- Arranque desde un CD/DVD. Consulte Descargar y grabar un CD or DVD de la imagen ISO del instalador de ESXi.
- Arranque desde una unidad flash USB. Consulte Formatear una unidad flash USB para arrancar la instalación o la actualización de ESXi.
- Arranque desde una red. Consulte Arranque de red del programa de instalación de ESXi.
- Arranque desde una ubicación remota mediante una aplicación de administración remota. Consulte Usar aplicaciones de administración remota.

Descargar y grabar un CD or DVD de la imagen ISO del instalador de ESXi

Si no tiene un CD/DVD de instalación de ESXi, puede crear uno.

También puede crear una imagen ISO del instalador que incluya un script de instalación personalizado. Consulte Crear una imagen ISO de instalador con un script de instalación o actualización personalizado.

Procedimiento

1 Siga el procedimiento descrito en Descarga del instalador de ESXi.

2 Grabe la imagen ISO en un CD o DVD.

Formatear una unidad flash USB para arrancar la instalación o la actualización de ESXi

Puede formatear una unidad flash USB para arrancar la instalación o la actualización de ESXi.

En las instrucciones de este procedimiento se supone que la unidad flash USB se detecta como `/dev/sdb`.

Nota El archivo `ks.cfg` que contiene el script de instalación no puede estar ubicado en la misma unidad flash USB que se utiliza para arrancar la instalación o la actualización. El archivo kickstart no depende del arranque BIOS o UEFI.

Requisitos previos

- Equipo Linux al que se acceda como superusuario
- Unidad flash USB que el equipo Linux pueda detectar
- La imagen ISO de ESXi, `VMware-VMvisor-Installer-`*`número_de_versión-número_de_compilación`*`.x86_64.iso`, que incluye el archivo `isolinux.cfg`

Procedimiento

1 Arranque Linux, inicie sesión e introduzca el modo de superusuario mediante un comando `su` o `sudo root`.

2 Si la unidad flash USB no se detecta como `/dev/sdb`, o si no conoce con certeza la forma en que se detecta la unidad flash USB, determine la manera en que se detecta.

   a Conecte la unidad flash USB.

   b En la línea de comandos, ejecute el comando para mostrar los mensajes de registro actuales.

   ```
   tail -f /var/log/messages
   ```

   Se mostrarán varios mensajes en los que se identifica la unidad flash USB con un formato similar al del siguiente mensaje.

   ```
   Oct 25 13:25:23 ubuntu kernel: [ 712.447080] sd 3:0:0:0: [sdb] Attached SCSI removable
   disk
   ```

   En este ejemplo, `sdb` identifica el dispositivo USB. Si su dispositivo se identifica de un modo diferente, use esa identificación en lugar de *sdb*.

3 Sobrescriba toda la unidad USB con la imagen ISO. Esto sobrescribe la tabla de particiones y todo el contenido anterior existente en la unidad USB.

   ```
   dd bs=10M if=VMware-VMvisor-Installer-version_number-build_number.x86_64.iso
   of=/dev/sdb
   ```

4 Expulsar la unidad USB.

   ```
   eject /dev/sdb
   ```

Resultados

Puede utilizar la unidad flash USB para arrancar el instalador de ESXi.

Crear una unidad flash USB para almacenar el script de instalación o actualización de ESXi

Puede utilizar una unidad flash USB para almacenar el script de instalación o actualización de ESXi que se va a utilizar para la instalación o actualización por script de ESXi.

Si existen varias unidades flash USB en el equipo de instalación, el software de instalación busca el script de instalación o actualización en todas las unidades flash USB que estén conectadas.

En las instrucciones de este procedimiento se supone que la unidad flash USB se detecta como `/dev/sdb`.

Nota No almacene el archivo `ks` que contiene el script de instalación o actualización en la misma unidad flash USB que se utiliza para arrancar la instalación o la actualización.

Requisitos previos

- Equipo Linux
- Script de instalación o actualización de ESXi, el archivo kickstart `ks.cfg`

- Unidad flash USB

Procedimiento

1. Conecte la unidad flash USB a un equipo Linux con acceso al script de instalación o actualización.
2. Cree una tabla de particiones.

   `/sbin/fdisk /dev/sdb`

   a. Escriba `d` para eliminar las particiones hasta que no quede ninguna.

   b. Escriba `n` para crear la partición principal 1 que abarca todo el disco.

   c. Escriba `t` para configurar el tipo para una configuración adecuada para el sistema de archivos FAT32, por ejemplo, **c**.

   d. Escriba `p` para imprimir la tabla de particiones.

   El resultado debe ser similar al texto siguiente:

   ```
   Disk /dev/sdb: 2004 MB, 2004877312 bytes
   255 heads, 63 sectors/track, 243 cylinders
   Units = cylinders of 16065 * 512 = 8225280 bytes
      Device Boot      Start         End      Blocks   Id  System
   /dev/sdb1             1           243      1951866  c   W95 FAT32 (LBA)
   ```

   e. Escriba `w` para escribir la tabla de particiones y salir.
3. Formatee la unidad flash USB con el sistema de archivos FAT32.

   `/sbin/mkfs.vfat -F 32 -n USB /dev/sdb1`
4. Cree un directorio de destino y monte la unidad flash USB allí.

   `mkdir -p /usbdisk`

   `mount /dev/sdb1 /usbdisk`
5. Copie el script de instalación de ESXi en la unidad flash USB.

   `cp ks.cfg /usbdisk`
6. Desmonte la unidad flash USB.

   `umount /usbdisk`

Resultados

La unidad flash USB contiene el script de instalación o actualización de ESXi.

Pasos siguientes

Al arrancar el instalador de ESXi, apunte a la ubicación de la unidad flash USB del script de instalación o actualización. Consulte Introducir las opciones de arranque para ejecutar un script de instalación o actualización y Archivos de configuración PXELINUX.

Crear una imagen ISO de instalador con un script de instalación o actualización personalizado

Puede personalizar la imagen ISO del instalador de ESXi estándar con su propio script de instalación o actualización. Esta personalización permite realizar una instalación o actualización desatendida y generada por script cuando arranque la imagen ISO del instalador resultante.

Consulte también Instalar ESXi mediante un script y Acerca del archivo boot.cfg .

Requisitos previos

- Equipo Linux
- La imagen ISO de ESXi `VMware-VMvisor-Installer-`*`x.x.x`*`-`*`XXXXXX`*`.x86_64.iso`, donde *`x.x.x`* es la versión de ESXi que está instalando y *`XXXXXX`* es el número de compilación de la imagen ISO del instalador
- Su script de instalación o actualización personalizado, el archivo de inicio de actividad `KS_CUST.CFG`

Procedimiento

1 Descargue la imagen ISO de ESXi desde el portal de soporte de Broadcom.

2 Monte la imagen ISO en una carpeta:

   `mount -o loop VMware-VMvisor-Installer-x.x.x-XXXXXX.x86_64.iso /esxi_cdrom_mount`

   `XXXXXX` es el número de versión de ESXi para la versión que está instalado o la versión a la que está actualizando.

3 Copie el contenido de `esxi_cdrom` en otra carpeta:

   `cp -r /esxi_cdrom_mount/* /esxi_cdrom`

4 Copie el archivo de inicio a `/esxi_cdrom`.

   `cp KS_CUST.CFG /esxi_cdrom`

5 Modifique el archivo `boot.cfg` tanto en `/esxi_cdrom/efi/boot/boot.cfg` (para arranque UEFI) como en `/esxi_cdrom/boot.cfg` (para arranque de BIOS heredado) para especificar la ubicación del script de instalación o actualización mediante la opción `kernelopt`.

   Debe utilizar caracteres en mayúscula para proporcionar la ruta de acceso del script, por ejemplo,

   ```
   kernelopt=runweasel ks=cdrom:/KS_CUST.CFG
   ```

   Este paso automatiza la instalación o la actualización, sin la necesidad de especificar el archivo de inicio durante este proceso.

6 Vuelva a crear la imagen ISO con el comando `mkisofs` o `genisoimage`.

Comando	Sintaxis
mkisofs	**mkisofs -relaxed-filenames -J -R -o custom_esxi.iso -b ISOLINUX.BIN -c BOOT.CAT -no-emul-boot -boot-load-size 4 -boot-info-table -eltorito-alt-boot -eltorito-platform efi -b EFIBOOT.IMG -no-emul-boot /esxi_cdrom**
genisoimage	**genisoimage -relaxed-filenames -J -R -o custom_esxi.iso -b ISOLINUX.BIN -c BOOT.CAT -no-emul-boot -boot-load-size 4 -boot-info-table -eltorito-alt-boot -e EFIBOOT.IMG -no-emul-boot /esxi_cdrom**

Esta imagen de instalador ISO se puede utilizar para un arranque normal o un arranque seguro UEFI. No obstante, vSphere Lifecycle Manager no puede comprobar la suma de comprobación de dicha imagen ISO y no puede utilizarse para las actualizaciones mediante flujos de trabajo de vSphere Lifecycle Manager.

Resultados

La imagen ISO incluye su script de instalación o actualización personalizado.

Pasos siguientes

Instale ESXi desde la imagen ISO.

Personalizar instalaciones con vSphere ESXi Image Builder

Se puede usar VMware vSphere®ESXi™ Image Builder CLI para crear imágenes de instalación de ESXi con un conjunto personalizado de actualizaciones, revisiones y controladores.

Se puede usar vSphere ESXi Image Builder con vSphere Client o con PowerCLI para crear una imagen de instalación de ESXi con un conjunto personalizado de actualizaciones y revisiones de ESXi. También se pueden incluir controladores de almacenamiento o red de otros fabricantes que se lancen entre versiones de vSphere.

Se puede implementar una imagen de ESXi creada con vSphere ESXi Image Builder de cualquiera de las siguientes maneras:

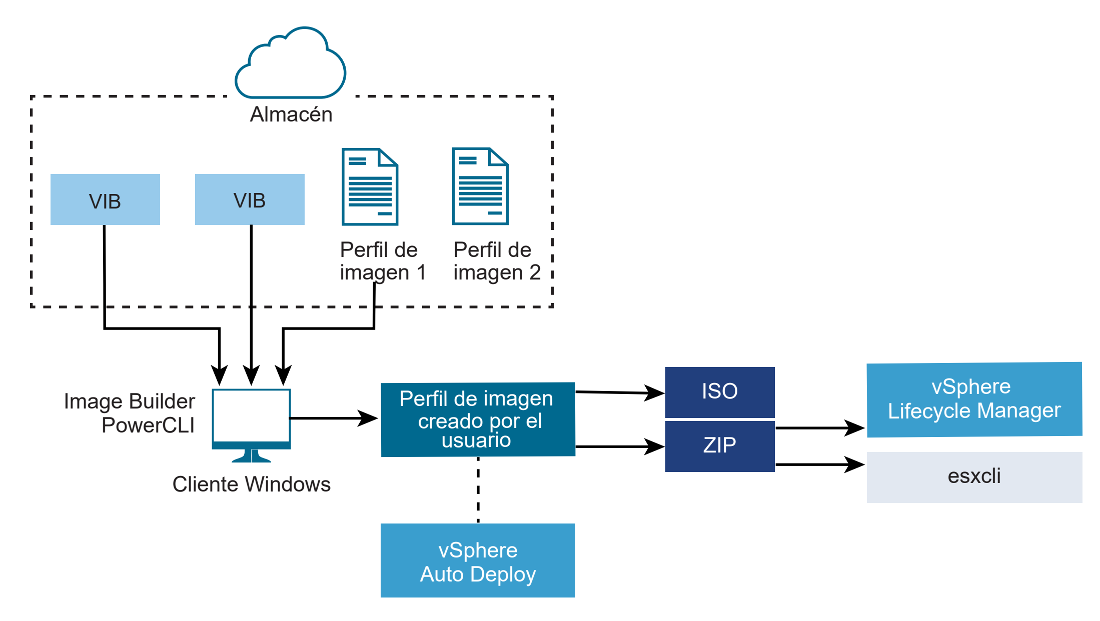
- Mediante la grabación de la imagen en un DVD de instalación.
- Mediante vCenter Server, utilizando la característica Auto Deploy.

Cómo funciona vSphere ESXi Image Builder

Cree perfiles de imagen ESXi para que los use vSphere Auto Deploy, agregue controladores de terceros personalizados a los perfiles de imagen y expórtelos o realice actualizaciones.

Con vSphere ESXi Image Builder puede crear perfiles de imagen ESXi para su uso por vSphere Auto Deploy, agregar controladores de terceros personalizados a perfiles de imagen existentes, exportar a ISO o paquete y realizar actualizaciones. Para conocer los conceptos básicos relacionados con la forma en que se crea, empaqueta y distribuye el software VMware vSphere, consulte Unidades de empaquetado de software que vSphere Lifecyle Manager puede consumir de la documentación Administración del ciclo de vida de hosts y clústeres.

Figura 4-2. Arquitectura de Image Builder



Puede usar cmdlets de vSphere ESXi Image Builder a fin de administrar el software para implementar en los hosts ESXi en varias situaciones diferentes.

Tabla 4-8. Casos en los que se puede utilizar vSphere ESXi Image Builder

Caso de uso para vSphere ESXi Image Builder	Descripción
Crear perfiles de imágenes para que use vSphere Auto Deploy	Use vSphere ESXi Image Builder para crear un perfil de imagen que defina los VIB que vSphere Auto Deploy emplea para aprovisionar hosts.
Agregar controladores de terceros personalizados a un perfil de imagen existente y exportarlos a un ISO o paquete	Cuando agregue un controlador de terceros o VIB personalizados de extensión a los hosts ESXi, use vSphere ESXi Image Builder para clonar la imagen base que proporcione VMware, agregue los VIB personalizados y expórtelos a un archivo ISO o un archivo ZIP en paquete sin conexión.
Realización de actualizaciones	Si actualiza un sistema que incluye extensiones o controladores personalizados, puede usar vSphere ESXi Image Builder para crear un perfil de imagen personalizado que incluya VIB compatibles con vSphere 8,0 para las extensiones personalizadas. Exporte el perfil de imagen personalizado a una imagen ISO o a un archivo ZIP para actualizar el sistema mediante líneas base de vSphere Lifecycle Manager.

Los cmdlets de vSphere ESXi Image Builder toman perfiles de imágenes y VIB como archivo de entrada y producen diversos archivos de salida.

Tabla 4-9. Archivos de entrada y salida de los cmdlets de vSphere ESXi Image Builder

Parámetro	Descripción
Archivo de entrada	Los perfiles de imágenes y los VIB se encuentran ubicados en un almacén de software y se usan como archivos de entrada para cmdlets de PowerCLI que se ejecutan en un cliente de Windows.
Archivos de salida	Los cmdlets de PowerCLI crean perfiles de imágenes personalizados que se pueden exportar a un archivo de imagen ISO o un archivo ZIP de almacén sin conexión. Para la instalación se usan imágenes ISO. El almacén de ZIP puede usarse mediante vSphere Lifecycle Manager o a través de comandos `esxcli software` para actualizar o instalar imágenes. Los perfiles de imágenes también se usan en reglas de vSphere Auto Deploy para personalizar el software con que se aprovisionan los hosts ESXi.

Vea el vídeo Uso de Image Builder CLI para obtener información sobre vSphere ESXi Image Builder:

 (Using Image Builder CLI)

Perfiles de imagen

Los perfiles de imagen definen el conjunto de VIB que utiliza un proceso de instalación o actualización de ESXi. Los perfiles de imagen se aplican a los hosts ESXi aprovisionados con vSphere Auto Deploy. El usuario define y manipula los perfiles de imagen con vSphere ESXi Image Builder.

Requisitos de los perfiles de imagen

Puede crear un perfil de imagen personalizado desde cero o clonar uno existente y agregarle o quitarle VIB. Para que sean válidos, los perfiles deben cumplir los siguientes requisitos.

- Cada perfil de imagen debe tener una combinación de nombre y proveedor única.
- Además, cada uno tiene un nivel de aceptación. Cuando agrega un VIB a un perfil de imagen con un cmdlet de vSphere ESXi Image Builder, este programa comprueba que el VIB coincida con el nivel de aceptación definido para el perfil.
- No puede quitar VIB que son necesarios para otros VIB.
- Tampoco puede incluir dos versiones del mismo VIB en un perfil de imagen. Cuando se agrega una nueva versión de un VIB, esta reemplaza a la versión existente.

Validar un perfil de imagen

Para que sean válidos, los perfiles de imagen y sus VIB deben cumplir varios criterios.

- Los perfiles de imagen deben contener al menos un VIB de base y un módulo de kernel de arranque.
- Si algún VIB del perfil de imagen depende de otro VIB, este otro también tendrá que estar incluido en el perfil de imagen. Los creadores de VIB almacenan esa información en la propiedad Depends del objeto SoftwarePackage.
- Los VIB no deben entrar en conflicto entre sí. Los creadores de VIB almacenan la información sobre conflictos en la propiedad Conflicts del objeto SoftwarePackage.
- Dos VIB con el mismo nombre, pero de dos versiones diferentes, no pueden coexistir. Cuando se agrega una nueva versión de un VIB, esta reemplaza a la versión existente.
- Hay problemas de falta de validación del nivel de aceptación.

Cuando se realiza un cambio en un perfil de imagen, vSphere ESXi Image Builder comprueba que el cambio no invalide el perfil.

Validación de dependencias

Cuando se agrega o se quita un VIB, vSphere ESXi Image Builder comprueba que se cumplan las dependencias del paquete. Cada objeto SoftwarePackage incluye una propiedad Depends que especifica una lista de otros VIB de los que depende ese VIB. Consulte Estructura de los objetos ImageProfile, SoftwarePackage e ImageProfileDiff

Validación del nivel de aceptación

vSphere ESXi Image Builder realiza una validación del nivel de aceptación cada vez que se crea o se modifica un perfil de imagen. vSphere ESXi Image Builder comprueba el nivel de aceptación de los VIB del perfil de imagen con el nivel de aceptación mínimo permitido del perfil. El nivel de aceptación del VIB también se valida cada vez que se valida la firma de un VIB.

Validar VIB durante la exportación

Cuando se exporta un perfil de imagen a una imagen ISO, vSphere ESXi Image Builder valida todos los VIB mediante las siguientes acciones.

- Comprueba que no haya conflictos mediante la comprobación de la propiedad Conflicts de todos los objetos SoftwarePackage.
- Realiza una validación de firma de VIB. La validación de la firma evita que se realicen modificaciones no autorizadas a los paquetes de VIB. La firma es una suma de comprobación criptográfica que garantiza que un determinado autor produjo el VIB. La validación de la firma también se lleva a cabo durante la instalación de VIB en un host ESXi y cuando el servidor vSphere Auto Deploy utiliza VIB.

- Comprueba que los VIB respeten las reglas de uso de rutas de archivo. VMware prueba los VIB VMwareCertified y VMwareAccepted para garantizar que estos respeten siempre las reglas de uso de rutas de archivo.

Trabajar con niveles de aceptación

Los hosts, los perfiles de imagen y los VIB individuales tienen niveles de aceptación. Los niveles de aceptación de VIB muestran cómo se probó el VIB. Como parte importante de los procedimientos de instalación y actualización, es necesario que comprenda lo que significa cada nivel de aceptación, cómo cambiar los niveles y qué implica cada cambio.

Los niveles de aceptación se configuran para hosts, perfiles de imagen y VIB individuales. El nivel de aceptación predeterminado para una imagen o un perfil de imagen de ESXi es PartnerSupported.

Niveles de aceptación de host

El nivel de aceptación de host determina qué VIB puede instalar en un host. Puede cambiar el nivel de aceptación de un host mediante los comandos ESXCLI. De forma predeterminada, los hosts ESXi tienen el nivel de aceptación PartnerSupported para permitir que se realicen actualizaciones fácilmente con los VIB PartnerSupported.

Nota VMware admite hosts con el nivel de aceptación PartnerSupported. Para conocer los problemas que podrían surgir con los VIB individuales con nivel de aceptación PartnerSupported, póngase en contacto con la organización de soporte del partner.

Niveles de aceptación de perfil de imagen

El nivel de aceptación de perfil de imagen se establece en el nivel de aceptación de VIB más bajo que haya en el perfil. Si desea agregar un VIB con un nivel de aceptación bajo a un perfil de imagen, puede cambiar el nivel de aceptación del perfil con el cmdlet `Set-EsxImageProfile`. Consulte Establecer el nivel de aceptación del perfil de imagen.

vSphere Lifecycle Manager no muestra el nivel de aceptación real. Utilice cmdlets de vSphere ESXi Image Builder para recuperar la información de nivel de aceptación para VIB y perfiles de imagen.

Niveles de aceptación de VIB

El nivel de aceptación de un VIB se establece cuando este se crea. Solo el creador del VIB puede establecer el nivel de aceptación.

Si intenta aprovisionar un host con un perfil de imagen o un VIB que tiene un nivel de aceptación más bajo que el host, se produce un error. Debe modificar el nivel de aceptación del host para instalar el perfil de imagen o el VIB. Consulte Cambiar nivel de aceptación del host. Al cambiar el nivel de aceptación del host, se modifica también su nivel de soporte.

El nivel de aceptación de un host, perfil de imagen o VIB permite determinar quién probó el VIB y quién lo admite. VMware admite los siguientes niveles de aceptación.

VMwareCertified

El nivel de aceptación VMwareCertified tiene los requisitos más estrictos. Los VIB con este nivel se someten a pruebas completamente equivalentes a las pruebas de control de calidad internas de VMware para la misma tecnología. Hoy en día, solo los controladores de los programas de proveedores de E/S (I/O Vendor Program, IOVP) se publican en este nivel. VMware responde a las llamadas de soporte para VIB con este nivel de aceptación.

VMwareAccepted

Los VIB con este nivel de aceptación pasan por pruebas de comprobación, pero estas no prueban completamente todas las funciones del software. El partner realiza pruebas y VMware comprueba el resultado. Hoy en día, los proveedores de CIM y los complementos de PSA son algunos de los VIB que se publican en este nivel. VMware indica a los clientes que realizan llamadas de soporte para VIB con este nivel de aceptación que se pongan en contacto con la organización de soporte del partner.

PartnerSupported

Los VIB con el nivel de aceptación PartnerSupported los publica un partner de confianza de VMware. El partner realiza todas las pruebas. VMware no comprueba los resultados. Este nivel se utiliza para una tecnología nueva o alternativa que los partners desean habilitar para los sistemas VMware. Hoy en día, las tecnologías de VIB de controlador, como Infiniband, ATAoE y SSD, se encuentran en este nivel con controladores de hardware que no son estándar. VMware indica a los clientes que realizan llamadas de soporte para VIB con este nivel de aceptación que se pongan en contacto con la organización de soporte del partner.

CommunitySupported

El nivel de aceptación CommunitySupported es para VIB creados por personas o empresas por fuera de los programas de partners de VMware. Los VIB de este nivel de aceptación no pasaron por un programa de pruebas aprobado por VMware y no son compatibles con el soporte técnico de VMware ni los partners de VMware.

Cambiar nivel de aceptación del host

Es posible disminuir el nivel de aceptación del host para que coincida con el de un VIB o un perfil de imagen que desea instalar.

El nivel de aceptación de cada VIB en un host debe ser por lo menos tan elevado como el nivel de aceptación del host. Por ejemplo, no es posible instalar un VIB con nivel de aceptación PartnerSupported en un host con nivel de aceptación VMwareAccepted. Primero debe disminuir el nivel de aceptación del host. Para obtener más información sobre los niveles de aceptación, consulte Trabajar con niveles de aceptación.

Advertencia El cambio del nivel de aceptación del host a CommunitySupported afecta la compatibilidad del host y podría perjudicar su seguridad.

Requisitos previos

Instale ESXCLI. Consulte *Introducción a ESXCLI*. Para solucionar problemas, ejecute comandos `esxcli` en ESXi Shell.

Procedimiento

1 Recupere el nivel de aceptación del VIB o el perfil de imagen.

Opción	Descripción
Ver información para todos los VIB	`esxcli --server=server_name software sources vib list --depot=depot_URL`
Ver información para un VIB específico	`esxcli --server=server_name software sources vib list --viburl=vib_URL`
Ver información para todos los perfiles de imagen	`esxcli --server=server_name software sources profile list --depot=depot_URL`
Ver información para un perfil de imagen específico	`esxcli --server=server_name software sources profile get --depot=depot_URL --profile=profile_name`

2 Vea el nivel de aceptación del host.

```
esxcli --server=server_name software acceptance get
```

3 Cambie el nivel de aceptación del host.

```
esxcli
                --server=server_name software acceptance set --level=acceptance_level
```

El valor de *nivel_de_aceptación* puede ser `VMwareCertified`, `VMwareAccepted`, `PartnerSupported` o `CommunitySupported`. Los valores para *nivel_de_aceptación* distinguen mayúsculas de minúsculas.

Nota Si el host tiene un nivel de aceptación más elevado que el VIB o el perfil de imagen que desea agregar, puede ejecutar comandos en el espacio de nombres `esxcli software vib` o `esxcli software profile` con la opción `--force`. Cuando utiliza la opción `--force`, aparece un mensaje de advertencia, ya que exige un VIB o un perfil de imagen con un nivel de aceptación más bajo que el del host y la configuración deja de ser coherente. La advertencia también aparece cuando instala VIB, elimina VIB o realiza ciertas otras operaciones en el host que tiene niveles de aceptación incoherentes.

Establecer el nivel de aceptación del perfil de imagen

Si desea agregar un VIB a un perfil de imagen, y el nivel de aceptación del VIB es menor al del perfil de imagen, puede clonar el perfil de imagen con un nivel de aceptación menor o cambiar el nivel de aceptación del perfil de imagen.

Puede especificar VMwareCertified, VMwareAccepted, PartnerSupported o CommunitySupported como un nivel de aceptación de un perfil de imagen. Si disminuye el nivel de aceptación, se cambiará el nivel de compatibilidad para el perfil de imagen y los hosts que aprovisiona con él. Para obtener más información, consulte Trabajar con niveles de aceptación.

Requisitos previos

Instale PowerCLI y todas las herramientas de software que constituyan un requisito previo. Consulte Configurar vSphere ESXi Image Builder .

Procedimiento

1 En una sesión de PowerCLI, ejecute el cmdlet `Add-EsxSoftwareDepot` para cada almacén con el que desea trabajar.

Opción	Acción
Almacén remoto	Ejecute `Add-EsxSoftwareDepot -DepotUrl <`*`url_del_almacén`*`>`.
Archivo ZIP	a Descargue el archivo ZIP en un sistema de archivos local. b Ejecute `Add-EsxSoftwareDepot -DepotUrl C:\<`*`file_path`*`>\<`*`offline-bundle`*`>.zip`

El cmdlet devuelve uno o más objetos `SoftwareDepot`.

2 Obtenga el nivel de aceptación para el perfil de imagen.

```
Get-EsxImageProfile -Name string
```

3 Establezca el nivel de aceptación del perfil de imagen.

```
Set-EsxImageProfile -Name string -AcceptanceLevel level
```

Estructura de los objetos ImageProfile, SoftwarePackage e ImageProfileDiff

Conocer la estructura de los objetos `ImageProfile`, `SoftwarePackage` y `ImageProfileDiff` ayuda a administrar los procesos de implementación y actualización.

Propiedades del objeto ImageProfile

El objeto `ImageProfile`, al que se puede acceder con el cmdlet de `Get-EsxImageProfile` PowerCLI, posee las siguientes propiedades.

Nombre	Tipo	Descripción
`AcceptanceLevel`	`AcceptanceLevel`	Determina qué VIB se pueden agregar al perfil. Los niveles son VMwareCertified, VMwareAccepted, PartnerSupported y CommunitySupported. Consulte Trabajar con niveles de aceptación.
`Author`	`System.String`	La persona que creó el perfil. 60 caracteres o menos.
`CreationTime`	`System.DateTime`	Marca de hora de creación.
`Description`	`System.String`	La descripción de texto completo del perfil. Sin límite de longitud.
`GUID`	`System.String`	Identificador único global del perfil de imagen.
`ModifiedTime`	`System.DateTime`	Marca de hora de la última modificación.
`Name`	`System.String`	Nombre del perfil de imagen. 80 caracteres o menos.
`ReadOnly`	`System.Boolean`	Cuando se establece en `true`, el perfil no se puede editar. Utilice `Set-EsxImageProfile -Readonly` para lograr que los perfiles de imagen personalizados sean de solo lectura.
`Rules`	`ImageProfileRule[]`	Cualquier restricción o requisito de hardware OEM que el perfil de imagen podría tener. vSphere Auto Deploy verifica el valor de esta propiedad al implementar un perfil de imagen, e implementa el perfil si se encuentra disponible hardware coincidente.
`Vendor`	`System.String`	La organización que publica el perfil. 40 caracteres o menos.
`VibList`	`SoftwarePackage[]`	La lista de identificadores de VIB que la imagen contiene.

Propiedades del objeto SoftwarePackage

Al preparar un perfil de imagen, puede examinar los paquetes de software para decidir qué paquetes son adecuados para la inclusión. El objeto `SoftwarePackage` posee las siguientes propiedades.

<table>
<tr><th>Nombre</th><th>Tipo</th><th>Descripción</th></tr>
<tr><td>AcceptanceLevel</td><td>AcceptanceLevel</td><td>El nivel de aceptación de este VIB.</td></tr>
<tr><td>Conflicts</td><td>SoftwareConstraint[]</td><td>Una lista de VIB que no se pueden instalar al mismo tiempo que este VIB. Cada limitación utiliza el siguiente formato:
package-name[<<|<=|=|>=|<< version]</td></tr>
<tr><td>Depends</td><td>SoftwareConstraint[]</td><td>Una lista de VIB que deben instalarse al mismo tiempo que este VIB. Mismo formato de limitación que la propiedad Conflicts.</td></tr>
<tr><td>Description</td><td>System.String</td><td>La descripción extensa de VIB.</td></tr>
<tr><td>Guid</td><td>System.String</td><td>El identificador único del VIB.</td></tr>
<tr><td>LiveInstallOk</td><td>System.Boolean</td><td>Valor “True” si se admiten las instalaciones activas en este VIB.</td></tr>
<tr><td>LiveRemoveOk</td><td>System.Boolean</td><td>Valor “True” si se admiten las eliminaciones activas en este VIB.</td></tr>
<tr><td>MaintenanceMode</td><td>System.Boolean</td><td>Valor “True” si los hosts deben estar en el modo de mantenimiento para la instalación de este VIB.</td></tr>
<tr><td>Name</td><td>System.String</td><td>Nombre del VIB. Generalmente describe de forma exclusiva al paquete en un sistema ESXi en ejecución.</td></tr>
<tr><td>Provides</td><td>SoftwareProvides</td><td>La lista de paquetes virtuales o interferencias que este VIB proporciona. Consulte Propiedades del objeto SoftwareProvide.</td></tr>
<tr><td>ReferenceURLs</td><td>SupportReference[]</td><td>La lista de objetos SupportReference con información de apoyo exhaustiva. El objeto SupportReference posee dos propiedades,Title y URL, ambas del tipo System.String.</td></tr>
<tr><td>Replaces</td><td>SoftwareConstraint[]</td><td>La lista de objetos SoftwareConstraint que identifica a los VIB que reemplazan a este VIB o lo vuelven obsoleto. Los VIB reemplazan automáticamente a los VIB con el mismo nombre, pero de versiones anteriores.</td></tr>
</table>

Nombre	Tipo	Descripción
ReleaseDate	System.DateTime	Fecha y hora de publicación o lanzamiento del VIB.
SourceUrls	System.String[]	La lista de URL de origen desde la que se puede descargar este VIB.
StatelessReady	System.Boolean	Valor “True” si el paquete es compatible con perfiles de host u otras tecnologías que permiten que sea adecuado para la utilización en conjunto con vSphere Auto Deploy.
Summary	System.String	Resumen de una línea del VIB.
Tags	System.String[]	Matriz de etiquetas de cadenas para este paquete definido por el proveedor o editor. Las etiquetas pueden utilizarse para identificar características del paquete.
Vendor	System.String	Proveedor o editor del VIB.
Version	System.String	Versión del VIB.
VersionObject	Software.Version	La propiedad `VersionObject` es del tipo `SoftwareVersion`. La clase `SoftwareVersion` implementa un método `Compare` estático para comparar dos versiones de cadenas. Consulte Propiedades del objeto SoftwareVersion

Propiedades del objeto ImageProfileDiff

Cuando ejecute el cmdlet `Compare-EsxImageProfile`, puede transferir dos parámetros, primero el perfil de referencia y, a continuación, el perfil de comparación. El cmdlet devuelve un objeto `ImageProfileDiff`, que posee las siguientes propiedades.

Nombre	Tipo	Descripción
CompAcceptanceLevel	System.String	El nivel de aceptación para el segundo perfil que se transfirió a `Compare-EsxImageProfile`.
DowngradeFromRef	System.String[]	La lista de VIB en el segundo perfil que son degradaciones de los VIB del primer perfil.
Equal	System.Boolean	Valor `True` si los dos perfiles de imagen poseen paquetes y niveles de aceptación idénticos.
OnlyInComp	System.String	La lista de VIB encontrados solo en el segundo perfil que se transfirió a `Compare-EsxImageProfile`.

Nombre	Tipo	Descripción
`OnlyInRef`	`System.String[]`	La lista de VIB encontrados solo en el primer perfil que se transfirió a `Compare-EsxImageProfile`.
`PackagesEqual`	`System.Boolean`	`True` si los perfiles de imagen poseen conjuntos idénticos de paquetes de VIB.
`RefAcceptanceLevel`	`System.String`	El nivel de aceptación para el primer perfil que se transfirió a `Compare-EsxImageProfile`.
`UpgradeFromRef`	`System.String[]`	La lista de VIB en el segundo perfil que son actualizaciones de los VIB del primer perfil.

Propiedades del objeto SoftwareVersion

El objeto `SoftwareVersion` permite comparar dos cadenas de versión. El objeto incluye un método `Compare` estático que acepta dos cadenas como entrada y devuelve `1` si la primera cadena de versión es un número superior a la segunda cadena de versión. `Compare` devuelve `0` si las dos cadenas de versión son iguales. `Compare`devuelve `-1` si la segunda cadena de versión es un número superior al de la primera cadena. El objeto posee las siguientes propiedades.

Nombre	Tipo	Descripción
`Version`	`System.String`	La parte de la versión antes del guión. Esta parte indica la versión principal.
`Release`	`System.String`	La parte de la versión después del guión. Esta parte indica la versión de la revisión.

Propiedades del objeto SoftwareConstraint

El objeto `SoftwareConstraint` implementa un método `MatchesProvide`. El método acepta un objeto `SoftwareProvides` o `SoftwarePackage` como entrada y devuelve `True` si la limitación coincide con `SoftwareProvide` o `SoftwarePackage` o, de lo contrario, devuelve `False`.

El objeto `SoftwareConstraint` posee las siguientes propiedades.

Nombre	Tipo	Descripción
`Name`	`System.String`	Nombre de la limitación. Este nombre debe coincidir con una propiedad `SoftwareProvideName` correspondiente.
`Relation`	`System.String`	Una enumeración o uno de los siguientes indicadores de comparación: <<, <=, = >=, >>. Esta propiedad puede ser $null si la limitación no posee una propiedad `Relation` y `Version`.

Nombre	Tipo	Descripción
`Version`	`System.String`	La versión para hacer coincidir la limitación. Esta propiedad puede ser $null si la limitación no posee una propiedad `Relation` y `Version`.
`VersionObject`	`SoftwareVersion`	La versión representada por un objeto `SoftwareVersion`.

Propiedades del objeto SoftwareProvide

El objeto `SoftwareProvide` posee las siguientes propiedades.

Nombre	Tipo	Descripción
`Name`	`System.String`	Nombre del suministro.
`Version`	`System.String`	Versión del suministro. Puede ser $null si el suministro no especifica una versión.
`Release`	`System.String`	La versión del suministro tal como se representa a través de un objeto SoftwareVersion. Consulte Propiedades del objeto SoftwareVersion.

Configurar vSphere ESXi Image Builder

Antes de que pueda ejecutar los cmdlets de vSphere ESXi Image Builder, deberá instalar PowerCLI y todo el software de requisito previo.

Requisitos previos

Antes de que pueda ejecutar los cmdlets de vSphere ESXi Image Builder, deberá instalar PowerCLI y todo el software de requisito previo. El complemento vSphere ESXi Image Builder se incluye con la instalación de PowerCLI. Si desea administrar vSphere ESXi Image Builder con cmdlets de PowerCLI, compruebe que Microsoft .NET Framework 4.5 o 4.5.x y Windows PowerShell 3.0 o 4.0 se encuentren instalados en un sistema Microsoft Windows. Consulte la Guía del usuario de PowerCLI.

Procedimiento

1 Abra PowerShell en su estación de trabajo.

2 Descargue una versión de PowerCLI posterior a PowerCLI 6.5R1 de la página de inicio de PowerCLI.

3 Para instalar todos los módulos de PowerCLI, ejecute el comando: `Install-Module VMware.PowerCLI -Scope CurrentUser`. Como alternativa, puede instalar módulos de PowerCLI individuales si ejecuta el cmdlet `Install-Module` con el nombre del módulo. Si aparece una advertencia de que está instalando módulos de un repositorio que no es de confianza, presione **y** y luego presione **Intro** para confirmar la instalación.

   Puede comprobar que el módulo de PowerCLI esté disponible mediante el comando

   `Get-Module -Name VMware.PowerCLI* -ListAvailable`.

Pasos siguientes

Revise Usar cmdlets de VMware.Image Builder . Si no está familiarizado con PowerCLI, lea la *Guía del usuario de PowerCLI*.

Utilice los cmdlets de vSphere ESXi Image Builder y otros cmdlets de PowerCLI y cmdlets de PowerShell para administrar los perfiles de imagen y VIB. Utilice `Get-Help` *nombre_del_cmdlet* en cualquier momento para obtener ayuda en la línea de comandos.

Configurar vSphere ESXi Image Builder

Antes de que pueda usar vSphere ESXi Image Builder con vSphere Client, debe comprobar que el servicio esté habilitado y en ejecución.

Requisitos previos

- Asegúrese de contar con suficiente espacio de almacenamiento para el repositorio de vSphere Auto Deploy. El servidor vSphere Auto Deploy utiliza el repositorio para almacenar los datos que necesita, incluidos las reglas y los conjuntos de reglas que usted crea, así como los VIB y los perfiles de imagen que se especifican en las reglas.

  Se recomienda asignar 2 GB para que haya suficiente espacio para almacenar cuatro perfiles de imagen y quede espacio adicional. Cada perfil de imagen requiere aproximadamente 400 MB. Determine la cantidad de perfiles de imagen que espera utilizar para definir la cantidad de espacio que debe reservar para el repositorio de vSphere Auto Deploy.

Procedimiento

1 Desplácese hasta **Inicio > Auto Deploy**.

   De forma predeterminada, solo la función de administrador tiene privilegios para usar el servicio vSphere Auto Deploy.

2 En la página **Auto Deploy**, seleccione la instancia de vCenter Server en el menú desplegable en la parte superior.

3 Haga clic en **Habilitar Image Builder** para activar el servicio.

   Aparecerá la página **Almacenes de software**.

Pasos siguientes

- Agregar un almacén de software.

- Importar un almacén de software.
- Clonar un perfil de imagen.
- Crear un perfil de imagen.
- Preparar el sistema para vSphere Auto Deploy.
- Puede cambiar las propiedades de configuración predeterminadas del **Servicio Image Builder**. Para obtener más información, consulte "Configurar vCenter Server" en la documentación de *Administrar vCenter Server y hosts*.

Usar cmdlets de VMware.Image Builder

Con los cmdlets de VMware.Image Builder, puede aprovechar todas las funciones de PowerCLI.

Los cmdlets de VMware.Image Builder se implementan como cmdlets de Microsoft PowerShell y se incluyen en PowerCLI. Puede aprovechar todas las funciones de PowerCLI mediante cmdlets de VMware.Image Builder. Los usuarios avanzados de PowerShell también pueden utilizar los cmdlets de VMware.Image Builder del mismo modo que otros cmdlets de PowerShell. Si estos son sus primeros pasos con PowerShell y PowerCLI, siga estos consejos.

Puede escribir cmdlets, parámetros y valores de parámetros en el shell de PowerCLI.

- Obtenga ayuda para cualquier cmdlet a través de `Get-Help` *`nombre_del_cmdlet`*.
- Recuerde que PowerShell no distingue mayúsculas de minúsculas.
- Utilice la opción de finalización con tabulación para los nombres de cmdlets y parámetros.
- Formatee cualquier variable y salida de cmdlet utilizando `Format-List` o `Format-Table` o sus formas cortas `fl` o `ft`. Consulte `Get-Help Format-List`.
- Utilice caracteres comodín para la búsqueda y filtrado de VIB y perfiles de imagen. Son compatibles todas las expresiones con comodines.

Transmitir parámetros por nombre

Puede transmitir parámetros por nombre en la mayoría de los casos y rodear los valores de parámetros que contienen espacios o caracteres especiales con comillas dobles.

```
Add-EsxSoftwarePackage -ImageProfile profile42 -SoftwarePackage "partner package 35"
```

Transmitir parámetros como objetos

Puede pasar los parámetros como objetos si desea realizar el scripting y automatización. Puede utilizar la técnica con cmdlets que devuelven varios objetos o con cmdlets que devuelven un solo objeto.

1 Asocie la salida de un cmdlet que devuelve varios objetos a una variable.

   ```
   $profs = Get-EsxImageProfile
   ```

2 Cuando ejecute el cmdlet que necesita el objeto como entrada, acceda al objeto por posición, con la lista comenzando con 0.

```
Add-EsxSoftwarePackage -ImageProfile $profs[4] -SoftwarePackage partner-pkg
```

El ejemplo agrega el paquete de software especificado al quinto perfil de imagen de la lista devuelto por `Get-EsxImageProfile`.

La mayoría de los ejemplos de la documentación *Instalar y configurar vCenter Server* pasan parámetros por nombre. Flujos de trabajo de vSphere ESXi Image Builder con cmdlets de PowerCLI incluye ejemplos que pasan parámetros como objetos.

Descripción general de los cmdlets de VMware.ImageBuilder

El componente VMware.Image Builder de VMware PowerCLI proporciona cmdlets para administrar VIB, perfiles de imagen y otro contenido en almacenes de software.

vSphere 7.0 y otras versiones posteriores introducen nuevas formas de empaquetar los VIB junto con boletines y revisiones heredados, y los almacenes de software contienen imágenes base, componentes y complementos de proveedor, junto con VIB y perfiles de imagen. VMware PowerCLI 12.0 y versiones posteriores proporcionan cmdlets que funcionan con el nuevo contenido existente en los almacenes de software.

VMware.ImageBuilder incluye los siguientes cmdlets.

Nota Al ejecutar cmdlets de VMware.ImageBuilder, proporcione todos los parámetros en la línea de comandos cuando invoque el cmdlet. No se recomienda proporcionar parámetros en modo interactivo.

Ejecute `Get-Help` *nombre_del_cmdlet* en el símbolo de PowerCLI para obtener información de referencia detallada.

Tabla 4-10. Cmdlets de VMware.ImageBuilder utilizados con contenido heredado en almacenes de software

Cmdlet	Descripción
`Add-EsxSoftwareDepot`	Agregar el almacén de software o el archivo ZIP en la ubicación especificada del entorno actual. Descarga metadatos del almacén y analiza los VIB para comprobar si tienen dependencias.
`Remove-EsxSoftwareDepot`	Se desconecta del almacén de software especificado.
`Get-EsxSoftwareDepot`	Devuelve una lista de almacenes de software que se encuentran en el entorno actual. Si desea examinar y administrar perfiles de imagen y VIB, primero debe agregar el almacén de software correspondiente al entorno.
`Get-EsxSoftwarePackage`	Devuelve una lista de objetos de paquete de software (VIB). Utilice estas opciones del cmdlet para filtrar los resultados.
`Get-EsxImageProfile`	Devuelve una matriz de objetos `ImageProfile` de todos los almacenes agregados actualmente.

Tabla 4-10. Cmdlets de VMware.ImageBuilder utilizados con contenido heredado en almacenes de software (continuación)

Cmdlet	Descripción
New-EsxImageProfile	Crea un nuevo perfil de imagen. En la mayoría de los casos, se recomienda crear un nuevo perfil mediante la clonación de un perfil existente. Consulte Clonar un perfil de imagen con cmdlets de PowerCLI.
Set-EsxImageProfile	Modifica un objeto ImageProfile local y realiza pruebas de validación en el perfil modificado. El cmdlet devuelve el objeto modificado pero no lo conserva.
Export-EsxImageProfile	Exporta un perfil de imagen como una imagen ISO de ESXi para instalar ESXi, o bien como un archivo ZIP.
Compare-EsxImageProfile	Devuelve una estructura ImageProfileDiff que muestra si dos perfiles tienen la misma lista de VIB y el mismo nivel de aceptación. Consulte Trabajar con niveles de aceptación.
Remove-EsxImageProfile	Elimina el perfil de imagen del almacén de software.
Add-EsxSoftwarePackage	Agrega uno o más paquetes (VIB) nuevos a un perfil de imagen existente.
Remove-EsxSoftwarePackage	Elimina uno o más paquetes (VIB) de un perfil de imagen.
Set-ESXImageProfileAssociation	Asocia el perfil de imagen especificado con el sistema ESXi especificado.

Tabla 4-11. Cmdlets de VMware.ImageBuilder utilizados con nuevo contenido en almacenes de software

Cmdlet	Descripción
Get-DepotAddons	Recupera una matriz de objetos que proporciona información básica sobre los complementos de un almacén de software.
Get-DepotBaseImages	Recupera una matriz de objetos que proporciona información básica sobre las imágenes base en un almacén de software.
Get-DepotComponents	Recupera una matriz de objetos que proporciona información básica sobre los componentes de un almacén de software.
Get-DepotInfo	Recupera información básica acerca del almacén de software ubicado en la ruta de archivos o la dirección URL especificada.
Get-DepotVibs	Recupera una matriz de objetos que proporciona información básica sobre los VIB en un almacén de software.
New-IsoImage	Genera una imagen ISO usando el almacén de software y la descripción de software especificados en la ruta de archivo indicada.
New-PxeImage	Genera una imagen PXE usando el almacén de software y la descripción de software especificados en la ruta de archivo indicada.

Tareas de perfil de imagen de ESXi

Manipule almacenes de software, perfiles de imagen y VIB mediante el componente de VMware.Image Builder de VMware PowerCLI o el vSphere Client.

Agregar un almacén de software

Agregue uno o varios almacenes de software al inventario de vSphere ESXi Image Builder para personalizar los perfiles de imagen.

Requisitos previos

Para poder trabajar con almacenes de software y personalizar perfiles de imagen, debe agregar uno o varios almacenes de software al inventario de vSphere ESXi Image Builder. Puede agregar un almacén de software utilizando vSphere Client.

Compruebe que el servicio vSphere ESXi Image Builder esté habilitado y en ejecución. Consulte Configurar vSphere ESXi Image Builder.

Procedimiento

1 Desplácese hasta **Inicio > Auto Deploy**.

   De forma predeterminada, solo la función de administrador tiene los privilegios para usar el servicio vSphere ESXi Image Builder.

2 En la pestaña **Almacenes de software**, haga clic en **Nuevo**.

   Aparecerá la ventana **Agregar almacén de software**.

3 Seleccione el tipo de almacén que desea crear.

Opción	Acción
Almacén en línea	a Escriba un nombre para el almacén en el inventario. b Introduzca la URL en el almacén en línea.
Almacén personalizado	Introduzca el nombre del almacén en el inventario.

   El almacén de software en línea de VMware se encuentra en https://hostupdate.vmware.com/software/VUM/PRODUCTION/main/vmw-depot-index.xml.

4 Haga clic en **Agregar**.

5 (opcional) Haga clic en la pestaña **Paquetes de software** para ver el contenido del almacén seleccionado y obtener información adicional sobre los paquetes.

6 (opcional) Si agrega un **Almacén en línea**, también es posible:

   - **Buscar actualizaciones** para obtener los paquetes de almacén más recientes.
   - Hacer clic en **Más información** para obtener detalles adicionales del almacén.

Resultados

El almacén de software se agrega a la lista.

Pasos siguientes

- Puede asociar un perfil de imagen con una nueva regla de vSphere Auto Deploy para aprovisionar hosts ESXi. Consulte Crear una regla de implementación o Clonar una regla de implementación.

- Puede asociar un perfil de imagen con un host ESXi. Consulte Agregar un host al inventario de vSphere Auto Deploy.
- Editar la asociación de perfil de imagen de un host.
- **Quitar** un almacén de software personalizado.

Importar un almacén de software

Si hay un almacén sin conexión ubicado en su sistema de archivos local, puede importar el archivo ZIP al inventario de vSphere ESXi Image Builder.

Requisitos previos

Si hay un almacén sin conexión ubicado en su sistema de archivos local, puede importar el archivo ZIP al inventario de vSphere ESXi Image Builder mediante vSphere Client.

Compruebe que el servicio vSphere ESXi Image Builder esté habilitado y en ejecución. Consulte Configurar vSphere ESXi Image Builder.

Procedimiento

1. Desplácese hasta **Inicio > Auto Deploy**.

   De forma predeterminada, solo la función de administrador tiene los privilegios para usar el servicio vSphere ESXi Image Builder.

2. En la pestaña **Almacenes de software**, haga clic en **Importar** .
3. Introduzca el nombre del almacén de software en el inventario.
4. Haga clic en **Examinar** y seleccione un archivo ZIP en el sistema local que contenga el almacén de software al que desea realizar la importación.
5. Haga clic en **Cargar**.

Pasos siguientes

- Puede asociar un perfil de imagen con una nueva regla de vSphere Auto Deploy para aprovisionar hosts ESXi. Consulte Crear una regla de implementación o Clonar una regla de implementación.
- Puede asociar un perfil de imagen con un host ESXi. Consulte Agregar un host al inventario de vSphere Auto Deploy.
- Editar la asociación de perfil de imagen de un host.

Clonar un perfil de imagen

Utilice vSphere Client para clonar perfiles de imagen.

Requisitos previos

Puede utilizar vSphere Client para clonar perfiles de imagen. Puede clonar un perfil de imagen cuando quiera realizar pequeños cambios en la lista de VIB de un perfil; o si quiere utilizar

hosts de distintos proveedores y quiere utilizar el mismo perfil básico, pero desea agregar VIB específicos de los proveedores.

- Compruebe que el servicio vSphere ESXi Image Builder esté habilitado y en ejecución. Consulte Configurar vSphere ESXi Image Builder.
- Agregue o importe un almacén de software al inventario de vSphere ESXi Image Builder. Consulte Agregar un almacén de software y Importar un almacén de software.
- Compruebe que exista al menos un almacén personalizado en el inventario de vSphere ESXi Image Builder.

Procedimiento

1 Desplácese hasta **Inicio > Auto Deploy**.

De forma predeterminada, solo la función de administrador tiene los privilegios para usar el servicio vSphere ESXi Image Builder.

2 En la pestaña **Almacenes de software**, use el menú desplegable para seleccionar el almacén de software que contiene el perfil de imagen con el que se trabajará.

3 En la lista de perfiles de imagen del almacén, seleccione el perfil de imagen que desea clonar y haga clic en **Clonar**.

4 Escriba un nombre de perfil de imagen, un proveedor y una descripción.

Debe escribir un nombre de perfil de imagen exclusivo.

5 En el menú desplegable **Almacén de software**, seleccione en qué almacén personalizado se agregará el nuevo perfil de imagen.

6 Haga clic en **Siguiente**.

Aparecerá la página **Seleccionar paquetes de software**.

7 En el menú desplegable, seleccione un nivel de aceptación para el perfil de imagen.

El nivel de aceptación de los VIB que se agregan a la imagen de base debe ser al menos tan alto como el de la imagen de base. Si agrega un VIB con un nivel de aceptación inferior al del perfil de imagen, debe reducir el nivel de aceptación del perfil de imagen. Para obtener más información, consulte Trabajar con niveles de aceptación.

8 Seleccione los VIB que quiere agregar al perfil de imagen y anule la selección de los que desea quitar; luego haga clic en **Siguiente**.

Nota El perfil de imagen debe contener una imagen de ESXi de arranque para ser válido.

vSphere ESXi Image Builder verifica que el cambio no invalide el perfil. Algunos VIB dependen de otros VIB y pierden su validez si se incluyen en un perfil de imagen por separado. Cuando se agrega o se quita un VIB, vSphere ESXi Image Builder comprueba si se cumplen las dependencias del paquete.

9 En la página **Listo para completar**, revise la información resumida del nuevo perfil de imagen y haga clic en **Finalizar**.

Pasos siguientes

- Puede asociar un perfil de imagen con una nueva regla de vSphere Auto Deploy para aprovisionar hosts ESXi. Consulte Crear una regla de implementación o Clonar una regla de implementación.
- Puede asociar un perfil de imagen con un host ESXi. Consulte Agregar un host al inventario de vSphere Auto Deploy.
- Editar la asociación de perfil de imagen de un host.

Clonar un perfil de imagen con cmdlets de PowerCLI

La clonación de un perfil publicado es la manera más sencilla de crear un perfil de imagen personalizado. La clonación de un perfil resulta especialmente útil si desea eliminar algunos VIB puntuales de un perfil, o si desea usar hosts de diferentes proveedores y quiere usar el mismo perfil básico, pero también agregar VIB de proveedores específicos. Las grandes instalaciones o los partners de VMware pueden considerar la posibilidad de crear un nuevo perfil.

Requisitos previos

- Instalar PowerCLI y todo el software necesario como requisito previo. Consulte Configurar vSphere ESXi Image Builder .
- Compruebe que tenga acceso al almacén de software que contiene el perfil de imagen que desea clonar.

Procedimiento

1 En una sesión de PowerCLI, ejecute el cmdlet `Add-EsxSoftwareDepot` para cada almacén con el que desea trabajar.

Opción	Acción
Almacén remoto	Ejecute `Add-EsxSoftwareDepot -DepotUrl <url_del_almacén>`.
Archivo ZIP	a Descargue el archivo ZIP en un sistema de archivos local. b Ejecute `Add-EsxSoftwareDepot -DepotUrl C:\<file_path>\<offline-bundle>.zip`

El cmdlet devuelve uno o más objetos `SoftwareDepot`.

2 (opcional) Ejecute el cmdlet `Get-EsxImageProfile` para buscar el nombre del perfil que desea clonar.

Puede utilizar opciones de filtros con `Get-EsxImageProfile`.

3 Ejecute el cmdlet `New-EsxImageProfile` para crear un nuevo perfil y use el parámetro `-CloneProfile` para especificar el perfil que desea clonar.

```
New-EsxImageProfile -CloneProfile My_Profile -Name "Test Profile 42"
```

En este ejemplo, se clona el perfil denominado *My_Profile* y se asigna el nombre Test Profile 42. Debe especificar una combinación exclusiva de nombre y proveedor para el perfil clonado.

Pasos siguientes

Consulte Revisar contenido de almacenes para ver algunos ejemplos de filtros.

Personalice el perfil de imagen agregando o eliminando VIB. Consulte Agregar VIB a un perfil de imagen con cmdlets de PowerCLI.

Crear un perfil de imagen

Puede crear un nuevo perfil de imagen a través de vSphere Client en lugar de clonar uno existente.

Requisitos previos

Podría considerar crear un nuevo perfil de imagen si este difiere de forma significativa de los perfiles de imagen de su inventario.

- Compruebe que el servicio vSphere ESXi Image Builder esté habilitado y en ejecución. Consulte Configurar vSphere ESXi Image Builder.
- Agregue o importe un almacén de software al inventario de vSphere ESXi Image Builder. Consulte Agregar un almacén de software y Importar un almacén de software.
- Compruebe que exista al menos un almacén personalizado en el inventario de vSphere ESXi Image Builder.

Procedimiento

1 Desplácese hasta **Inicio > Auto Deploy**.

   De forma predeterminada, solo la función de administrador tiene los privilegios para usar el servicio vSphere ESXi Image Builder.

2 En el menú desplegable **Almacén de software**, seleccione en qué almacén personalizado se agregará el nuevo perfil de imagen.

3 En la pestaña Perfiles de imagen, haga clic en **Nuevo perfil de imagen**.

4 Escriba un nombre de perfil de imagen, un proveedor y una descripción.

   Debe escribir un nombre de perfil de imagen exclusivo.

5 Haga clic en **Siguiente**.

   Aparecerá la página **Seleccionar paquetes de software**.

6 En el menú desplegable, seleccione un nivel de aceptación para el perfil de imagen.

El nivel de aceptación de los VIB que se agregan a la imagen de base debe ser al menos tan alto como el de la imagen de base. Si agrega un VIB con un nivel de aceptación inferior al del perfil de imagen, debe reducir el nivel de aceptación del perfil de imagen. Para obtener más información, consulte Trabajar con niveles de aceptación.

7 Seleccione los VIB que quiere agregar al perfil de imagen y anule la selección de los que desea quitar; luego haga clic en **Siguiente**.

Nota El perfil de imagen debe contener una imagen de ESXi de arranque para ser válido.

vSphere ESXi Image Builder verifica que el cambio no invalide el perfil. Algunos VIB dependen de otros VIB y pierden su validez si se incluyen en un perfil de imagen por separado. Cuando se agrega o se quita un VIB, vSphere ESXi Image Builder comprueba si se cumplen las dependencias del paquete.

8 En la página **Listo para completar**, revise la información resumida del nuevo perfil de imagen y haga clic en **Finalizar**.

Pasos siguientes

- Puede asociar un perfil de imagen con una nueva regla de vSphere Auto Deploy para aprovisionar hosts ESXi. Consulte Crear una regla de implementación o Clonar una regla de implementación.
- Puede asociar un perfil de imagen con un host ESXi. Consulte Agregar un host al inventario de vSphere Auto Deploy.
- Editar la asociación de perfil de imagen de un host.
- Seleccione y **elimine** un perfil de imagen.
- **Ver paquetes de software** para el perfil de imagen seleccionado.

Crear una imagen ISO de ESXi personalizada con cmdlets de PowerCLI

Con ESXi Image Builder, puede personalizar un perfil de imagen ESXi, pero no combinar contenido de diferentes almacenes para generar una imagen ISO. A partir de VMware PowerCLI 12.0, puede personalizar imágenes ISO mediante el contenido de varios almacenes de software y una especificación de software personalizada.

El cmdlet `New-IsoImage` conserva los metadatos adicionales que requiere vSphere Lifecycle Manager, como la imagen base, el complemento y el componente. Estos metadatos adicionales no forman parte de las imágenes ISO que se pueden exportar mediante los cmdlets de ESXi Image Builder heredados.

Requisitos previos

Instale VMware PowerCLI 12.0 o una versión posterior.

Compruebe que tiene acceso al almacén de software que contiene la especificación de software que desea utilizar.

Procedimiento

1 Recopile la información necesaria para la especificación de software que utiliza para crear una imagen ISO personalizada.

a Obtenga la versión de la imagen base para la revisión o actualización requerida ejecutando el cmdlet `Get-DepotBaseImages`:

```
PS C:\> Get-DepotBaseImages -Depot C:\VMware-ESXi-8.xxx-xxxxxxxx-depot.zip
```

La salida del comando es:

```
Version                                  Vendor
Release date
-------                                  ------
------------
8.0.0-0.0.xxxxxx                       VMware, Inc.
01/01/20xx 00:00:00
```

b Obtenga otros paquetes, como complementos de OEM, con cmdlets utilizados con nuevos metadatos en almacenes de software. Por ejemplo:

```
PS C:\> Get-DepotAddons -Depot C:\addon-depot.zip
```

La salida del comando es:

```
Name                    Version                 ID
Vendor                  Release date
----                    -------                 --
------                  ------------
testaddonv1             1.0.0-1                 testaddonv1:1.0.0-1     ESXLifecycle
QE         02/20/20xx 18:28:23
```

Con el cmdlet `Get-DepotComponents` también puede enumerar todos los componentes existentes en un almacén de software:

```
PS C:\> Get-DepotComponents -Depot C:\Intel-i40en_1.12.3.0-1OEM.xxxxxxx.zip
```

La salida del comando es:

```
Name                                 Version
ID                                                  Vendor
----                                 -------
--                                                 ------
Intel-i40en                          1.12.3.0-1OEM.xxxxxxx   Intel-
i40en:1.12.3.0-1OEM.xxxxxxx         Intel
```

Puede usar cualquier número y combinación de almacenes de software en línea y sin conexión.

2 Cree una especificación de software. Por ejemplo:

```
{
    "base_image": {
        "version": "8.0.0-0.0.xxxxxxx"
    },
    "add_on": {
        "name": "testaddonv1",
        "version": "1.0.0-1"
    },
    "components": {
      "Intel-i40en": "1.12.3.0-1OEM.xxxxxxx"
   }
}
```

La especificación de software es un archivo JSON que contiene información acerca de la imagen base de ESXi y paquetes adicionales, como un complemento del proveedor.

3 Genere una imagen ISO personalizada ejecutando el cmdlet `New-IsoImage` con los parámetros `Depots`, `SoftwareSpec` y `Destination`. Por ejemplo:

```
New-IsoImage -Depots "c:\temp\VMware-ESXi-8.0-xxxxxxx-depot.zip" , "c:\temp\HPE-xxxxxxx-Jan20xx-Synergy-Addon-depot.zip" -SoftwareSpec "c:\temp\HPE-80xx-custom.JSON" -Destination "c:\temp\HPE-80xx-custom.iso"
```

Los almacenes incluyen la ruta de acceso a los archivos ZIP para la versión de ESXi compatible y el complemento del proveedor. El destino incluye la ruta de acceso y el nombre de archivo del archivo ISO personalizado.

Puede transferir opciones de kernel adicionales, crear una imagen en vivo, sobrescribir los archivos existentes o comprobar los niveles de aceptación para los VIB individuales que se utilizaron durante la creación de la imagen. Para obtener más información acerca del cmdlet `New-IsoImage`, consulte https://code.vmware.com/docs/11794/cmdletreference/doc/New-IsoImage.html.

Pasos siguientes

Puede importar la nueva imagen ISO al almacén de vSphere Lifecycle Manager, de modo que pueda crear líneas base de actualización que utilizará en las operaciones de actualización de host.

Crear una imagen PXE personalizada con cmdlets de PowerCLI

A partir de VMware PowerCLI 12.0, puede crear una imagen PXE personalizada mediante cualquier almacén de software y una especificación de software personalizada.

Requisitos previos

Instale VMware PowerCLI 12.0 o una versión posterior.

Compruebe que tiene acceso al almacén de software que contiene la especificación de software que desea utilizar.

Procedimiento

1 Recopile la información necesaria para la especificación de software que utiliza para crear una imagen PXE personalizada.

a Obtenga la versión de la imagen base para la revisión o actualización requerida ejecutando el cmdlet `Get-DepotBaseImages`:

```
PS C:\> Get-DepotBaseImages -Depot C:\VMware-ESXi-8.xxxx-xxxxx-depot.zip
```

La salida del comando es:

```
Version                                 Vendor
Release date
-------                                 ------
------------
8.x.x.xxx.xxxxx                      VMware, Inc.
04/29/20xx 00:00:00
```

b Obtenga otros paquetes, como complementos de OEM, con cmdlets utilizados con nuevos metadatos en almacenes de software. Por ejemplo:

```
PS C:\> Get-DepotAddons -Depot C:\addon-depot.zip
```

La salida del comando es:

```
Name                    Version                 ID
Vendor                  Release date
----                    -------                 --
------                  ------------
testaddonv1             1.0.0-1                 testaddonv1:1.0.0-1     ESXLifecycle
QE         02/20/20xx 18:28:23
```

Con el cmdlet `Get-DepotComponents` también puede enumerar todos los componentes existentes en un almacén de software:

```
PS C:\> Get-DepotComponents -Depot C:\Intel-
i40en_1.12.3.0-1OEM.700.1.0.15843807_18058526.zip
```

La salida del comando es:

```
Name                             Version
ID                                                Vendor
----                             -------
--                                             ------
Intel-i40en                      1.12.3.0-1OEM.xxxxx   Intel-i40en:1.12.3.0-1OEM.xxxxx
Intel
```

Puede usar cualquier número y combinación de almacenes de software en línea y sin conexión.

2 Cree una especificación de software. Por ejemplo:

```
{
    "base_image": {
        "version": "8.0.xxxxx"
    },
    "add_on": {
        "name": "testaddonv1",
        "version": "1.0.0-1"
    },
    "components": {
      "Intel-i40en": "1.12.3.0-1OEM.xxxxx"
   }
}
```

La especificación de software es un archivo JSON que contiene información acerca de la imagen base de ESXi y paquetes adicionales, como un complemento del proveedor.

3 Genere una imagen PXE personalizada ejecutando el cmdlet `New-PxeImage` con los parámetros `Depots`, `SoftwareSpec` y `Destination`. Por ejemplo:

```
New-PxeImage -Depots "c:\temp\VMware-ESXi-8.0xxxxx-xxxxx-depot.zip" ,
"c:\temp\HPE-8.0xxxxx-xxx-Synergy-Addon-depot.zip" -SoftwareSpec "c:\temp\HPE-xxx-
custom.JSON" -Destination "C:\pxe-image"
```

Los almacenes incluyen la ruta de acceso a los archivos ZIP para la versión de ESXi compatible y el complemento del proveedor. El destino incluye la ruta y el nombre de archivo del archivo PXE personalizado.

Puede transferir opciones de kernel adicionales, crear una imagen en vivo, sobrescribir los archivos existentes o comprobar los niveles de aceptación para los VIB individuales que se utilizaron durante la creación de la imagen. Para obtener más información acerca del cmdlet `New-PxeImage`, consulte https://code.vmware.com/docs/11794/cmdletreference/doc/New-PxeImage.html.

Pasos siguientes

Puede utilizar la imagen PXE en los flujos de trabajo de corrección de hosts ESXi con arranque PXE.

Editar un perfil de imagen

Puede editar perfiles de imagen mediante vSphere Client. Puede cambiar el nombre, los detalles y la lista VIB de un perfil de imagen.

Requisitos previos

- Compruebe que el servicio vSphere ESXi Image Builder esté habilitado y en ejecución. Consulte Configurar vSphere ESXi Image Builder.
- Agregue o importe un almacén de software al inventario de vSphere ESXi Image Builder. Consulte Agregar un almacén de software y Importar un almacén de software.

- Compruebe que exista al menos un almacén personalizado en el inventario de vSphere ESXi Image Builder.

Procedimiento

1. Desplácese hasta **Inicio > Auto Deploy**.

   De forma predeterminada, solo la función de administrador tiene los privilegios para usar el servicio vSphere ESXi Image Builder.

2. En la pestaña **Almacenes de software**, use el menú desplegable para seleccionar el almacén de software que contiene el perfil de imagen con el que se trabajará.

3. En la pestaña **Perfiles de imagen**, seleccione el perfil de imagen que desea editar y haga clic en **Editar**.

   Aparecerá el asistente **Editar perfil de imagen**.

4. (opcional) Cambie el nombre, el proveedor y la información de la descripción del perfil de imagen.

5. Haga clic en **Siguiente**.

   Aparecerá la página **Seleccionar paquetes de software**.

6. En el menú desplegable, seleccione un nivel de aceptación para el perfil de imagen.

   El nivel de aceptación de los VIB que se agregan a la imagen de base debe ser al menos tan alto como el de la imagen de base. Si agrega un VIB con un nivel de aceptación inferior al del perfil de imagen, debe reducir el nivel de aceptación del perfil de imagen. Para obtener más información, consulte Trabajar con niveles de aceptación.

7. Seleccione los VIB que quiere agregar al perfil de imagen y anule la selección de los que desea quitar; luego haga clic en **Siguiente**.

   Nota El perfil de imagen debe contener una imagen de ESXi de arranque para ser válido.

   vSphere ESXi Image Builder verifica que el cambio no invalide el perfil. Algunos VIB dependen de otros VIB y pierden su validez si se incluyen en un perfil de imagen por separado. Cuando se agrega o se quita un VIB, vSphere ESXi Image Builder comprueba si se cumplen las dependencias del paquete.

8. En la página **Listo para completar**, revise la información resumida del perfil de imagen editado y haga clic en **Finalizar**.

Pasos siguientes

- Puede asociar un perfil de imagen con una nueva regla de vSphere Auto Deploy para aprovisionar hosts ESXi. Consulte Crear una regla de implementación o Clonar una regla de implementación.
- Puede asociar un perfil de imagen con un host ESXi. Consulte Agregar un host al inventario de vSphere Auto Deploy.

- Editar la asociación de perfil de imagen de un host.

Agregar VIB a un perfil de imagen con cmdlets de PowerCLI

Puede agregar uno o más VIB a un perfil de imagen si dicho perfil de imagen no está configurado en solo lectura. Si el nuevo VIB depende de otros VIB o entra en conflicto con otros VIB del perfil, aparecerá un mensaje en el símbolo del sistema de PowerShell y no se agregará el VIB.

Puede agregar VIB desde VMware o desde partners de VMware a un perfil de imagen. Si agrega VIB de VMware, vSphere ESXi Image Builder realiza la validación. Si agrega VIB desde uno o más partners OEM de forma simultánea, no se informa de errores, pero el perfil de imagen resultante podría no funcionar. Instale los VIB desde solo un proveedor OEM al mismo tiempo.

Si aparece un error sobre problemas con el nivel de aceptación, cambie el nivel de aceptación del perfil de imagen y el nivel de aceptación del host. Considere meticulosamente si es apropiado el cambio del nivel de aceptación del host. Los niveles de aceptación de VIB se establecen durante la creación del VIB y no se pueden cambiar.

Puede agregar los VIB incluso si el perfil de imagen resultante no es válido.

Nota VMware solo puede admitir entornos y configuraciones que hayan demostrado ser estables y totalmente funcionales a través de pruebas rigurosas y exhaustivas. Utilice solo aquellas configuraciones compatibles. Puede utilizar VIB personalizados si reduce el nivel de aceptación del host y, como resultado, la compatibilidad. En dicho caso, registre los cambios realizados, a fin de que pueda revertirlos en caso de que desee eliminar los VIB personalizados y restaurar posteriormente el nivel de aceptación del host al valor predeterminado (Partner Supported). Consulte Trabajar con niveles de aceptación.

Requisitos previos

Instalar PowerCLI y todo el software necesario como requisito previo. Consulte Configurar vSphere ESXi Image Builder

Procedimiento

1 En una sesión de PowerCLI, ejecute el cmdlet `Add-EsxSoftwareDepot` para cada almacén con el que desea trabajar.

Opción	Acción
Almacén remoto	Ejecute `Add-EsxSoftwareDepot -DepotUrl` *<url_del_almacén>*.
Archivo ZIP	a Descargue el archivo ZIP en un sistema de archivos local. b Ejecute `Add-EsxSoftwareDepot -DepotUrl C:\`*<file_path>*`\`*<offline-bundle>*`.zip`

El cmdlet devuelve uno o más objetos `SoftwareDepot`.

2 Ejecute el cmdlet `Get-EsxImageProfile` para mostrar todos los perfiles de imagen de todos los almacenes actualmente visibles.

   El cmdlet devuelve todos los perfiles disponibles. Puede limitar la búsqueda utilizando los argumentos opcionales para filtrar la salida.

3 Clone el perfil.

```
New-EsxImageProfile -CloneProfile My_Profile -Name "Test Profile 42" -Vendor "My Vendor"
```

   Los perfiles de imagen publicados por VMware y sus partners son de solo lectura. Para realizar cambios, deberá clonar el perfil de imagen. Se requiere el parámetro `vendor`.

4 Ejecute el cmdlet `Add-EsxSoftwarePackage` para agregar un paquete nuevo a uno de los perfiles de imagen.

```
Add-EsxSoftwarePackage -ImageProfile My_Profile -SoftwarePackage partner-package
```

   El cmdlet ejecuta las pruebas de validación estándares en el perfil de imagen. Si la validación es correcta, el cmdlet devuelve un perfil de imagen modificado y validado. Si el VIB que desea agregar depende de un VIB diferente, el cmdlet muestra dicha información e incluye el VIB que puede resolver la dependencia. Si el nivel de aceptación del VIB que desea agregar es inferior al nivel de aceptación del perfil de imagen, ocurrirá un error.

Comparar perfiles de imagen

Puede comparar dos perfiles de imagen a través de vSphere Client para comprobar si poseen la misma lista de VIB, versión o nivel de aceptación.

Requisitos previos

- Compruebe que el servicio vSphere ESXi Image Builder esté habilitado y en ejecución. Consulte Configurar vSphere ESXi Image Builder.
- Agregue o importe un almacén de software al inventario de vSphere ESXi Image Builder. Consulte Agregar un almacén de software y Importar un almacén de software.

Procedimiento

1 Desplácese hasta **Inicio > Auto Deploy**.

   De forma predeterminada, solo la función de administrador tiene los privilegios para usar el servicio vSphere ESXi Image Builder.

2 En la pestaña **Almacenes de software**, use el menú desplegable para seleccionar el almacén de software que contiene el perfil de imagen con el que se trabajará.

3 En la pestaña **Perfiles de imagen**, seleccione un perfil de imagen y haga clic en **Comparar con**.

   Aparecerá el asistente **Comparar perfil de imagen**.

4 Haga clic en **Cambiar** para seleccionar un segundo perfil de imagen.

   Aparecerá la página **Seleccionar perfil de imagen**.

5 Seleccione un almacén de software en el menú desplegable y haga clic en el segundo perfil de imagen.

6 En la página **Comparar perfil de imagen**, seleccione una opción de comparación en el menú desplegable **Paquetes de software**.

   En la parte izquierda de la lista, se muestran los detalles de los VIB que contiene el primer perfil de imagen seleccionado. En la parte derecha de la lista se proporciona información sobre el segundo perfil de imagen. Los VIB marcados como `Mismo` son idénticos en ambos perfiles. Para los VIB presentes en uno de los perfiles de imagen, está marcada la opción `Ausente` junto al perfil de imagen donde no están presentes.

Comparar perfiles de imagen con cmdlets de PowerCLI

Puede comparar dos perfiles de imagen a través del cmdlet `Compare-EsxImageProfile`, por ejemplo, para comprobar si poseen la misma lista de VIB o nivel de aceptación. También es posible la comparación de perfiles de imagen o sus propiedades utilizando los operadores de comparación de PowerShell.

Requisitos previos

Instalar PowerCLI y todo el software necesario como requisito previo. Consulte Configurar vSphere ESXi Image Builder .

Procedimiento

1 En una sesión de PowerCLI, ejecute el cmdlet `Add-EsxSoftwareDepot` para cada almacén con el que desea trabajar.

Opción	Acción
Almacén remoto	Ejecute `Add-EsxSoftwareDepot -DepotUrl <url_del_almacén>`.
Archivo ZIP	a Descargue el archivo ZIP en un sistema de archivos local. b Ejecute `Add-EsxSoftwareDepot -DepotUrl C:\<file_path>\<offline-bundle>.zip`

   El cmdlet devuelve uno o más objetos `SoftwareDepot`.

2 (opcional) Ejecute el cmdlet `Get-EsxImageProfile` para visualizar una lista de todos los perfiles de imagen en todos los almacenes disponibles.

   En la lista, puede encontrar los nombres de los perfiles de imagen que desea comparar.

3 Antes de comparar los perfiles de imagen, asígnelos a variables.

Por ejemplo, puede crear las variables `$imageProfile1` y `$imageProfile2` para conservar los nombres de los perfiles de imagen comparados.

```
$imageProfile1
                = Get-EsxImageProfile -Name "ImageProfile1"
$imageProfile2
                = Get-EsxImageProfile -Name "ImageProfile2"
```

4 Compare los dos perfiles de imagen a través del cmdlet `Compare-EsxImageProfile` o el operador de comparación `-eq`, que devuelve un valor booleano.

- Compare los dos perfiles de imagen para obtener una descripción completa de las diferencias a través del cmdlet `Compare-EsxImageProfile`.

```
Compare-EsxImageProfile -ReferenceProfile
                     $imageProfile1 -ComparisonProfile $imageProfile2
```

- Compare los dos perfiles de imagen por lista de VIB y nivel de aceptación a través del operador de comparación `-eq`.

```
if ($imageProfile1 -eq $imageProfile2) {
   Write-host "Successfully verified that both image profiles are equal."
} else {
   Write-host "Failed to verify that the image profiles are equal."
}
```

- Compare los dos perfiles de imagen por una propiedad específica a través del operador de comparación `-eq`.

```
if ($imageProfile1.vendor -eq $imageProfile2.vendor) {
   Write-host "Successfully verified that both image profiles are equal."
} else {
   Write-host "Failed to verify that the image profiles are equal."
}
```

Mover un perfil de imagen a un almacén de software distinto

Puede mover perfiles de imagen entre almacenes personalizados mediante vSphere Client y modificarlos sin afectar a la configuración del almacén de origen.

Requisitos previos

- Compruebe que el servicio vSphere ESXi Image Builder esté habilitado y en ejecución. Consulte Configurar vSphere ESXi Image Builder.
- Agregue o importe un almacén de software al inventario de vSphere ESXi Image Builder. Consulte Agregar un almacén de software y Importar un almacén de software.
- Compruebe que exista al menos un almacén personalizado en el inventario de vSphere ESXi Image Builder.

Procedimiento

1 Desplácese hasta **Inicio > Auto Deploy**.

De forma predeterminada, solo la función de administrador tiene los privilegios para usar el servicio vSphere ESXi Image Builder.

2 En la pestaña **Almacenes de software**, use el menú desplegable para seleccionar el almacén de software que contiene el perfil de imagen con el que se trabajará.

3 En la pestaña **Perfiles de imagen**, seleccione uno de ellos y haga clic en **Mover a**.

4 En el menú desplegable, seleccione el almacén personalizado adonde quiere mover el perfil de imagen.

5 Haga clic en **Aceptar**.

Resultados

El perfil de imagen se encuentra en el nuevo almacén de software.

Exportar un perfil de imagen a ISO o ZIP de paquete sin conexión

Puede exportar un perfil de imagen a una imagen ISO o un archivo ZIP mediante vSphere Client.

Requisitos previos

Puede exportar un perfil de imagen a una imagen ISO o un archivo ZIP mediante vSphere Client. Puede utilizar la imagen ISO como instalador de ESXi o para actualizar los hosts con vSphere Lifecycle Manager. El archivo ZIP contiene metadatos y los VIB del perfil de imagen. Puede utilizarlo para las actualizaciones de ESXi o como almacén sin conexión.

- Compruebe que el servicio vSphere ESXi Image Builder esté habilitado y en ejecución. Consulte Configurar vSphere ESXi Image Builder.
- Agregue o importe un almacén de software al inventario de vSphere ESXi Image Builder. Consulte Agregar un almacén de software y Importar un almacén de software.

Procedimiento

1 Desplácese hasta **Inicio > Auto Deploy**.

De forma predeterminada, solo la función de administrador tiene los privilegios para usar el servicio vSphere ESXi Image Builder.

2 En la pestaña **Almacenes de software**, use el menú desplegable para seleccionar el almacén de software que contiene el perfil de imagen con el que se trabajará.

3 En la pestaña **Perfiles de imagen**, seleccione el perfil de imagen que quiere exportar y haga clic en **Exportar**.

Aparecerá la ventana **Exportar perfil de imagen**.

4 Seleccione el tipo del archivo exportado.

Opción	Descripción
ISO	Exporta el perfil de imagen a una imagen ISO de arranque. Si desea crear una imagen ISO que se pueda grabar en un CD o DVD, y que se pueda utilizar para iniciar una instancia de ESXi sin estado, active la casilla **No incluya un instalador en la imagen ISO**.
ZIP	Exporta el perfil de imagen a un archivo ZIP.

5 (opcional) Si desea omitir la verificación del nivel de aceptación del perfil de imagen, seleccione **Omitir comprobación de firma de perfil de imagen**.

6 Haga clic en **Aceptar**.

El vínculo **Descargar** comienza a generarse en la columna "Descargar perfiles de imagen" del perfil de imagen seleccionado.

7 Cuando la imagen termine de generarse correctamente, haga clic en **Descargar** para guardar el archivo exportado.

Pasos siguientes

- Puede asociar un perfil de imagen con una nueva regla de vSphere Auto Deploy para aprovisionar hosts ESXi. Consulte Crear una regla de implementación o Clonar una regla de implementación.
- Puede asociar un perfil de imagen con un host ESXi. Consulte Agregar un host al inventario de vSphere Auto Deploy.
- Editar la asociación de perfil de imagen de un host.

Exportar un perfil de imagen a un ISO o un ZIP de paquete sin conexión con cmdlets de PowerCLI

Puede exportar un perfil de imagen a una imagen ISO o un archivo ZIP que contenga archivos y carpetas de componentes. No puede crear los dos si ejecuta el cmdlet una sola vez. Puede utilizar una imagen ISO como el instalador de ESXi o cargar la imagen ISO a vSphere Lifecycle Manager para actualizaciones.

Requisitos previos

Instalar PowerCLI y todo el software necesario como requisito previo. Consulte Configurar vSphere ESXi Image Builder .

Procedimiento

1 En una sesión de PowerCLI, ejecute el cmdlet `Add-EsxSoftwareDepot` para cada almacén con el que desea trabajar.

Opción	Acción
Almacén remoto	Ejecute `Add-EsxSoftwareDepot -DepotUrl <url_del_almacén>`.
Archivo ZIP	a Descargue el archivo ZIP en un sistema de archivos local. b Ejecute `Add-EsxSoftwareDepot -DepotUrl C:\<file_path>\<offline-bundle>.zip`

El cmdlet devuelve uno o más objetos `SoftwareDepot`.

2 Ejecute `Export-EsxImageProfile` para exportar el perfil de imagen.

Formato de exportación	Cmdlet
Imágenes ISO	`Export-EsxImageProfile` con el parámetro `-ExportToIso`
Archivos ZIP de almacén sin conexión	`Export-EsxImageProfile` con el parámetro `-ExportToBundle`

Resultados

Para la imagen ISO, vSphere ESXi Image Builder valida firmas de VIB, agrega archivos binarios de VIB a la imagen y descarga la imagen a la ubicación especificada. Para el archivo ZIP, vSphere ESXi Image Builder valida firmas de VIB y descarga los archivos binarios de VIB a la ubicación especificada.

Ejemplo: Exportar un perfil de imagen

Siga estos pasos para exportar un perfil de imagen a una imagen ISO.

1 Agregue el almacén de software.

```
Add-EsxSoftwareDepot -DepotUrl url_or_file
```

2 Observe todos los perfiles de imagen disponibles para encontrar el nombre del perfil de imagen que desea exportar.

```
Get-EsxImageProfile
```

3 Exporte el perfil de imagen.

```
Export-EsxImageProfile -ImageProfile "myprofile" -ExportToIso -FilePath iso_name
```

Siga estos pasos para exportar un perfil de imagen a un archivo ZIP que contenga archivos y carpetas de componentes.

1 Agregue el almacén de software.

```
Add-EsxSoftwareDepot -DepotUrl url_or_file
```

2 Observe todos los perfiles de imagen disponibles para encontrar el nombre del perfil de imagen que desea exportar.

```
Get-EsxImageProfile
```

3 Exporte el perfil de imagen.

```
Export-EsxImageProfile -ImageProfile "myprofile" -ExportToBundle -FilePath C:\my_bundle.zip
```

Pasos siguientes

Utilice la imagen ISO en una instalación de ESXi o cargue la imagen ISO a vSphere Lifecycle Manager para realizar actualizaciones.

Utilice el archivo ZIP para actualizar una instalación de ESXi.

- Importe el archivo ZIP en vSphere Lifecycle Manager para utilizarlo con líneas base de revisión.
- Descargue el archivo ZIP a un host ESXi o un almacén de datos, y ejecute los comandos `esxcli software vib` para importar los VIB del archivo ZIP.

Consulte la documentación de *Actualizar vSphere*.

Regenerar un perfil de imagen

Si utiliza Auto Deploy para agregar hosts ESXi con estado a un clúster que haya administrado mediante una imagen, debe asegurarse de que todos los hosts tengan la misma especificación de software.

Cuando se crea una regla de Auto Deploy y una imagen administra el clúster de destino, se crea una imagen de entorno de ejecución de prearranque (Preboot Execution Environment, PXE) en función de la especificación de la imagen del clúster. La imagen PXE generada se almacena en caché y no se actualiza automáticamente. Como resultado, si modifica la especificación de la imagen en vSphere Lifecycle Manager, debe actualizar la imagen PXE manualmente.

Para obtener información sobre cómo crear una regla para agregar hosts a un clúster administrado por una imagen, consulte *Usar Auto Deploy para agregar un host a un clúster administrado por una imagen* en la documentación de *vSphere Lifecycle Manager*.

Requisitos previos

Procedimiento

1 Desplácese hasta **Inicio > Auto Deploy**.

   De forma predeterminada, solo la función de administrador tiene privilegios para usar el servicio vSphere Auto Deploy.

2 En la pestaña **Reglas de implementación**, seleccione la regla que desee.

   Debe seleccionar una regla que empareje a los hosts ESXi con un clúster que administre mediante una imagen.

3 Si la regla está activa, primero debe desactivarla.

   a Haga clic en la pestaña **Activar/desactivar reglas**

   b En el cuadro de diálogo , seleccione la regla.

   c En el cuadro de diálogo , seleccione **Desactivar** y haga clic en **Aceptar**.

4 Seleccione **Volver a crear perfil de imagen** y, en el cuadro de diálogo de confirmación, haga clic en **Volver a crear**.

5 (opcional) Active la regla de nuevo.

   a Haga clic en la pestaña **Activar/desactivar reglas**

   b En el cuadro de diálogo , seleccione la regla.

   c En el cuadro de diálogo , seleccione **Activar** y haga clic en **Aceptar**.

Resultados

La imagen PXE se ejecuta con la especificación de imagen más reciente.

Conservar perfiles de imagen en todas las sesiones con PowerCLI

Puede exportar el perfil de imagen a un almacén de software de archivos zip y agregar ese depósito en la siguiente sesión.

Requisitos previos

Cuando se crea un perfil de imagen y se sale de la sesión de PowerCLI, el perfil de imagen ya no está disponible cuando se inicia una nueva sesión. Puede exportar el perfil de imagen a un almacén de software de archivos zip y agregar ese depósito en la siguiente sesión.

Instalar PowerCLI y todo el software necesario como requisito previo. Consulte Configurar vSphere ESXi Image Builder .

Procedimiento

1 En una sesión de PowerCLI, cree un perfil de imagen, por ejemplo, clonando un perfil de imagen existente y agregando un VIB.

2 Exporte el perfil de imagen a un archivo ZIP llamando a `Export-EsxImageProfile` con el parámetro `ExportToBundle`.

```
Export-EsxImageProfile    -ImageProfile "my_profile" -ExportToBundle -FilePath
                "C:\isos\temp-base-plus-vib25.zip"
```

3 Salga de la sesión de PowerCLI.

4 Cuando inicie una nueva sesión de PowerCLI, agregue el almacén que contiene su perfil de imagen para poder acceder a él.

```
Add-EsxSoftwareDepot "C:\isos\temp-base-plus-vib25.zip"
```

Comparar VIB con cmdlets de PowerCLI

Puede comparar dos VIB o sus propiedades usando los operadores de comparación de PowerShell.

Requisitos previos

Instalar PowerCLI y todo el software necesario como requisito previo. Consulte Configurar vSphere ESXi Image Builder .

Procedimiento

1 En una sesión de PowerCLI, ejecute el cmdlet Add-EsxSoftwareDepot para cada almacén con el que desea trabajar.

Opción	Acción
Almacén remoto	Ejecute Add-EsxSoftwareDepot -DepotUrl <*url_del_almacén*>.
Archivo ZIP	a Descargue el archivo ZIP en un sistema de archivos local. b Ejecute Add-EsxSoftwareDepot -DepotUrl C:\<*file_path*>\<*offline-bundle*>.zip

El cmdlet devuelve uno o más objetos SoftwareDepot.

2 (opcional) Ejecute el cmdlet Get-EsxSoftwarePackage para ver todos los VIB disponibles.

En la lista, puede encontrar los nombres de los VIB que desea comparar.

3 Antes de comparar los VIB, asígnelos a variables.

Por ejemplo, puede crear las variables $vib1 y $vib2 para mantener los nombre de los VIB comparados.

```
$vib1 = Get-EsxSoftwarePackage -Name "ReferenceVIB"
$vib2 = Get-EsxSoftwarePackage -Name "ComparisonVIB"
```

4 Use un operador de comparación para comparar los VIB por contenido y nivel de aceptación, o por una propiedad específica.

- Compare los dos VIB según su contenido y nivel de aceptación.

```
if ($vib1 -eq $vib2) {
   Write-host "Successfully verified that both VIBs are equal."
} else {
   Write-host "Failed to verify that the VIBs are equal."
}
```

- Compare una propiedad específica de los VIB usando un operador de comparación, como `-eq`, `-lt`, `-le`, `-gt` o `-ge`.

  ```
  if ($vib1.VersionObject -lt $vib2.VersionObject) {
     Write-host "Successfully verified that both the VIBs are equal."
  } else {
     Write-host "Failed to verify that the VIBs are equal."
  }
  ```

Flujos de trabajo de vSphere ESXi Image Builder con cmdlets de PowerCLI

Los flujos de trabajo de vSphere ESXi Image Builder son ejemplos de uso de cmdlets y no representan tareas reales.

Los flujos de trabajo de vSphere ESXi Image Builder son ejemplos del uso de cmdlets. Los flujos de trabajo no representan tareas reales, sino que ilustran cómo se pueden explorar diferentes maneras de usar un cmdlet. Los administradores que prueban los flujos de trabajo se benefician mediante una experiencia con PowerCLI, con Microsoft PowerShell o con ambos.

Revisar contenido de almacenes

Puede examinar los almacenes de software y los VIB con cmdlets de vSphere ESXi Image Builder mediante todo tipo de expresiones comodín.

El propio flujo de trabajo transmite los parámetros por nombre. No obstante, es posible acceder a variables para transmitir parámetros como objetos.

Puede utilizar opciones de filtros y expresiones con comodines para examinar el contenido de los almacenes.

Requisitos previos

Compruebe que PowerCLI y el software requerido estén instalados. Consulte Configurar vSphere ESXi Image Builder .

Procedimiento

1 En una sesión de PowerCLI, ejecute el cmdlet `Add-EsxSoftwareDepot` para cada almacén con el que desea trabajar.

Opción	Acción
Almacén remoto	Ejecute `Add-EsxSoftwareDepot -DepotUrl` *<url_del_almacén>*.
Archivo ZIP	a Descargue el archivo ZIP en un sistema de archivos local. b Ejecute `Add-EsxSoftwareDepot -DepotUrl C:\`*<file_path>*`\`*<offline-bundle>*`.zip`

El cmdlet devuelve uno o más objetos `SoftwareDepot`.

2 Recupere los perfiles de imagen.

Puede filtrarlos por proveedor, nombre y nivel de aceptación.

- ```
  Get-EsxImageProfiles
  ```

  Devuelve una matriz de objetos de `ImageProfile` provenientes de todos los almacenes que se agregaron a la sesión.

- ```
  Get-EsxImageProfile -Vendor "C*"
  ```

  Devuelve todos los perfiles de imagen creados por un proveedor cuyo nombre comienza con la letra C.

3 Recupere los paquetes de software mediante el cmdlet `Get-EsxSoftwarePackage`.

Puede filtrarlos (por ejemplo, por proveedor o versión) y puede usar los caracteres comodín estándar de PowerShell.

- ```
  Get-EsxSoftwarePackage -Vendor "V*"
  ```

  Devuelve todos los paquetes de software de un proveedor cuyo nombre comienza con la letra V.

- ```
  Get-EsxSoftwarePackage -Vendor "V*" -Name "*scsi*"
  ```

  Devuelve todos los paquetes de software cuyo nombre contiene la cadena `scsi` y que pertenecen a un proveedor cuyo nombre comienza con la letra V.

- ```
  Get-EsxSoftwarePackage -Version "2.0*"
  ```

  Devuelve todos los paquetes de software con una cadena de versión que comienza con 2.0.

4 Use `-Newest` para buscar el paquete más reciente.

- ```
  Get-EsxSoftwarePackage -Vendor "V*" -Newest
  ```

  Devuelve el paquete más reciente para los proveedores cuyo nombre comienza con la letra V y muestra la información mediante una tabla.

- ```
  Get-EsxSoftwarePackage -Vendor "V*" -Newest | format-list
  ```

  Devuelve información detallada acerca de cada paquete de software, mediante un canal que permite enlazar el resultado de la solicitud de paquetes de software emitida al cmdlet `format-list` de PowerShell.

5 Vea la lista de VIB en el perfil de imagen.

```
(Get-EsxImageProfile -Name "Robin's Profile").VibList
```

`VibList` es una propiedad del objeto `ImageProfile`.
```

6 Recupere los paquetes de software lanzados antes o después de una fecha determinada, mediante los parámetros `CreatedBefore` o `CreatedAfter`.

```
Get-EsxSoftwarePackage -CreatedAfter 7/1/2010
```

Ejemplo: Revisar el contenido de almacenes mediante variables

En este ejemplo de flujo de trabajo, se examina el contenido de un almacén mediante la transmisión de parámetros como objetos a los que se accede por posición en una variable, no mediante la transmisión de parámetros por nombre. Puede ejecutar los comandos siguientes en una secuencia desde la línea de comandos de PowerCLI. Reemplace los nombres por nombres que resulten adecuados para la instalación correspondiente.

```
Get-EsxSoftwarePackage -Vendor "V*"
Get-EsxSoftwarePackage -Vendor "V*" -Name "r*"
Get-EsxSoftwarePackage -Version "2.0*"
$ip1 = Get-EsxImageProfile -name ESX-5.0.0-123456-full
$ip1.VibList
Get-EsxSoftwarePackage -CreatedAfter 7/1/2010
```

Crear perfiles de imagen a través de un flujo de trabajo de clonación

Use cmdlets de vSphere ESXi Image Builder para comprobar los almacenes disponibles, agregar un almacén, ver la información del perfil de imagen y clonar un nuevo perfil de imagen.

Los perfiles publicados generalmente son de solo lectura y no pueden modificarse. Incluso si un perfil publicado no es de solo lectura, clonar en lugar de modificar el perfil es la práctica recomendada, debido a que la modificación de un perfil original elimina el original. No podrá revertir al perfil original no modificado, excepto si realiza una reconexión con un almacén.

Un flujo de trabajo de clonación de perfiles podría incluir comprobar el estado actual del sistema, agregar un almacén de software y clonar el perfil.

Requisitos previos

Puede utilizar los cmdlets de vSphere ESXi Image Builder para comprobar los almacenes que están disponibles, agregar un almacén, visualizar la información de un perfil de imagen y crear un perfil de imagen nuevo mediante la clonación de uno de los perfiles de imagen disponibles.

Compruebe que PowerCLI y el software requerido estén instalados. Consulte Configurar vSphere ESXi Image Builder .

Procedimiento

1 En una ventana de PowerShell, compruebe si se ha definido algún almacén de software para la sesión actual.

```
$DefaultSoftwareDepots
```

PowerShell devuelve los almacenes definidos actualmente o nada si se acaba de iniciar PowerShell.

2 Si el almacén que contiene el perfil que desea clonar no aparece en los resultados, agréguelo a la sesión actual.

Opción	Acción
Almacén remoto	Ejecute `Add-EsxSoftwareDepot -DepotUrl` *`url_del_almacén`*.
Archivo ZIP	a Descargue el archivo ZIP en la ruta de acceso de archivo local. b Ejecute `Add-EsxSoftwareDepot -DepotUrl C:\ruta_al_archivo\`*`offline-bundle`*`.zip`

PowerShell agregará el almacén especificado a la sesión actual y mostrará todos los almacenes actuales.

3 (opcional) Compruebe la variable `$DefaultSoftwareDepots`, que ahora devuelve el almacén recientemente agregado.

4 Vea todos los perfiles de imagen disponibles.

```
Get-EsxImageProfile
```

5 Para clonar un perfil de imagen, introduzca su nombre, un nombre nuevo para el perfil nuevo y un nombre para el proveedor.

```
$ip = New-EsxImageProfile -CloneProfile base-tbd-v1 -Name "Test Profile 42" -Vendor
"Vendor20"
```

6 (opcional) Visualice el perfil de imagen recientemente creado, `$ip`.

PowerShell devuelve la información sobre el perfil de imagen en formato tabular.

```
Name                Vendor          Last Modified          Acceptance Level
----                ------          -------------          ----------------
Test Profile 42     Vendor20        9/15/2010 5:45:43...   PartnerSupported
```

Ejemplo: Crear un perfil de imagen mediante la clonación con variables

En este ejemplo de flujo de trabajo, se repiten los pasos de este flujo de trabajo mediante la transmisión de parámetros como objetos a los que se accede por posición en una variable, no mediante la transmisión de parámetros por nombre. Puede ejecutar los siguientes cmdlets en secuencia desde la línea de comandos de PowerCLI.

```
$DefaultSoftwareDepots
Add-EsxSoftwareDepot -DepotUrl depot_url
$DefaultSoftwareDepots
$profs = Get-EsxImageProfile
$profs
$ip = New-EsxImageProfile -CloneProfile $profs[2] -Name "new_profile_name" -Vendor "my_vendor"
$ip
```

Crear flujos de trabajo de nuevos perfiles de imagen

Puede clonar un perfil de imagen existente o crear un nuevo perfil de imagen, para el cual debe definir dependencias y niveles de aceptación.

El sistema espera que el nivel de aceptación de los VIB que se agregan a la imagen de base sea igual de alto que el nivel de la imagen de base. Si se tiene que agregar un VIB con un nivel de aceptación menor al perfil de imagen, se debe bajar el nivel de aceptación del perfil de imagen. Para obtener más información, consulte Establecer el nivel de aceptación del perfil de imagen.

Como alternativa a la especificación de los parámetros en la línea de comandos, se puede usar el mecanismo de introducción de información de PowerShell para especificar parámetros de cadena. La introducción de información no funciona para otros parámetros, como objetos.

Requisitos previos

En la mayoría de las situaciones, se crea un perfil de imagen clonando un perfil existente. Es posible que algunos clientes o partners de VMware necesiten crear un nuevo perfil de imagen. Ponga mucha atención a las dependencias y a los niveles de aceptación en caso de que se cree un perfil de imagen desde cero.

- PowerCLI y el software de requisito previo están instalados. Consulte Configurar vSphere ESXi Image Builder .
- Tiene acceso a un almacén que incluye una imagen base y uno o más VIB. Los partners de VMware y VMware tienen almacenes públicos a los que se accede mediante URL. Los partners de VMware o VMware pueden crear un archivo ZIP que se puede descomprimir en el entorno local y al que se puede acceder mediante una ruta de acceso de archivo.

Procedimiento

1 En una sesión de PowerCLI, ejecute el cmdlet Add-EsxSoftwareDepot para cada almacén con el que desea trabajar.

Opción	Acción
Almacén remoto	Ejecute Add-EsxSoftwareDepot -DepotUrl <*url_del_almacén*>.
Archivo ZIP	a Descargue el archivo ZIP en un sistema de archivos local. b Ejecute Add-EsxSoftwareDepot -DepotUrl C:\<*file_path*>\<*offline-bundle*>.zip

El cmdlet devuelve uno o más objetos SoftwareDepot.

2 Ejecute el cmdlet Get-EsxImageProfile para mostrar todos los perfiles de imagen de todos los almacenes actualmente visibles. Puede limitar la búsqueda utilizando los argumentos opcionales para filtrar la salida.

```
Get-EsxSoftwarePackage -CreatedAfter 7/1/2010
```

3 Cree un nuevo perfil, asígnele un nombre y proveedor y agregue un paquete base.

```
New-EsxImageProfile -NewProfile -Name "Test #2" -vendor "Vendor42" -SoftwarePackage esx-
base[0],esx-xlibs[0]
```

El ejemplo usa el paquete esx-base. En la mayoría de los casos, cuando se crea un nuevo perfil de imagen se incluye el paquete esx-base. Los nombres que contienen espacios van con comillas.

4 Use un proceso para pasar el nuevo perfil de imagen a `format-list` para obtener información detallada sobre el nuevo paquete.

```
(Get-EsxImageProfile -Name "Test #2").VibList | format-list
```

Ejemplo: Crear perfiles de imagen desde cero utilizando variables

Esta secuencia de comandos repite los pasos del flujo de trabajo, pero pasa parámetros como objetos, a los que se accede mediante posición en una variable, en lugar de pasar parámetros por nombre. Se pueden ejecutar los siguientes comandos en secuencia en el mensaje PowerCLI.

```
Add-EsxSoftwareDepot depoturl
$pkgs = Get-EsxSoftwarePackage -CreatedAfter 7/1/2010
$ip2 = New-EsxImageProfile -NewProfile -Name "Test #2" -vendor "Vendor42" -SoftwarePackage
$pkgs[0]
$ip2.VibList | format-list
```

Editar flujo de trabajo de perfiles de imagen

Puede crear una imagen personalizada mediante la clonación y edición de un perfil de imagen utilizando PowerCLI.

Requisitos previos

Puede crear una imagen personalizada mediante la clonación y edición de un perfil de imagen utilizando PowerCLI. Puede agregar o eliminar uno o varios VIB en el perfil existente. Si agregar o eliminar VIB evita que el perfil de imagen funcione de forma correcta, se generará un error.

- PowerCLI y el software de requisito previo están instalados. Consulte Configurar vSphere ESXi Image Builder .
- Tiene acceso a un almacén que incluye una imagen base y uno o más VIB. VMware y partners de VMware permiten que estén disponibles almacenes públicos a los que se puede acceder a través de una dirección URL. VMware o partners de VMware pueden crear un archivo ZIP que puede descargar a su entorno local y acceder a través de una ruta de archivo.

Procedimiento

1 En una sesión de PowerCLI, ejecute el cmdlet `Add-EsxSoftwareDepot` para cada almacén con el que desea trabajar.

Opción	Acción
Almacén remoto	Ejecute `Add-EsxSoftwareDepot -DepotUrl <url_del_almacén>`.
Archivo ZIP	a Descargue el archivo ZIP en un sistema de archivos local. b Ejecute `Add-EsxSoftwareDepot -DepotUrl C:\<file_path>\<offline-bundle>.zip`

El cmdlet devuelve uno o más objetos `SoftwareDepot`.

2 Utilice una canalización para pasar el perfil de imagen que desea editar a `format-list` para acceder a información detallada.

En este ejemplo, el perfil de imagen creado en Crear flujos de trabajo de nuevos perfiles de imagen contiene solo la imagen base. No se incluye en el almacén un perfil de imagen nuevo creado. En cambio, puede acceder al perfil de imagen por el nombre o mediante la asociación con una variable.

```
Get-EsxImageProfile "Test #2" | format-list
```

PowerShell devuelve la información.

```
Name                : Test #2
Vendor               : Vendor42
...
VibList              : {esx-base 5.0.0.-...,}
```

3 (opcional) Si va a agregar un VIB con un nivel de aceptación inferior que aquel del perfil de imagen, cambie el nivel de aceptación del perfil de imagen.

```
Set-EsxImageProfile -ImageProfile "Test #2" -AcceptanceLevel VMwareAccepted
```

PowerShell devuelve la información sobre el perfil cambiado en formato tabular.

```
Name           Vendor           Last Modified       Acceptance Level
----           ------           -------------       ----------------
Test #2        Vendor42         9/22/2010 12:05:... VMwareAccepted
```

4 Agregue un paquete de software (VIB) al perfil de imagen. Puede agregar el paquete por nombre.

```
Add-EsxSoftwarePackage -ImageProfile "Test #2"
                -SoftwarePackage NewPack3
```

PowerShell devuelve la información sobre el perfil de imagen en formato tabular.

```
Name            Vendor           Last Modified       Acceptance Level
----            ------           -------------       ----------------
Test #2         Vendor42         9/22/2010 12:05:... VMwareAccepted
```

Nota Si ocurre un error cuando agrega el paquete de software, es posible que tenga un problema con los niveles de aceptación. Consulte Trabajar con niveles de aceptación

5 Vuelva a visualizar el perfil de imagen.

```
Get-EsxImageProfile "Test #2" | format-list
```

La lista de VIB se actualiza para incluir el paquete de software nuevo y se muestra la información.

```
Name                : Test #2
Vendor               : Vendor42
...
VibList              : {esx-base 5.0.0.-..., NewPack3}
```

Ejemplo: Editar perfiles de imagen a través de variables

Esta secuencia de cmdlet repite los pasos del flujo de trabajo, pero pasa los parámetros como objetos, a los que se accede a través de una posición en una variable, en lugar de pasar los parámetros por nombre. Puede ejecutar los siguientes cmdlets en secuencia desde la línea de comandos de PowerCLI.

```
Add-EsxSoftwareDepot -DepotUrl depot_url
$ip2 = Get-EsxImageProfile -name "Test #2"
$ip2 | format-list
Set-EsxImageProfile -ImageProfile $ip2 -AcceptanceLevel VMwareAccepted
Add-EsxImageSoftwarePackage -ImageProfile $ip2 -SoftwarePackage NewPack3
$ip2 | format-list
```

Instalación de ESXi

Puede instalar ESXi de forma interactiva, con una instalación generada por script o con vSphere Auto Deploy.

Instalar ESXi de forma interactiva

Utilice la opción de instalación interactiva para implementaciones pequeñas con menos de cinco hosts.

En una instalación interactiva típica, debe arrancar el instalador de ESXi y responder las solicitudes para instalar ESXi en el disco host local. El instalador vuelve a formatear y particiona el disco de destino y, a continuación, instala la imagen de arranque de ESXi. Si no instaló ESXi en el disco de destino antes, se sobrescribirán todos los datos de la unidad. Esto incluye las particiones de proveedores de hardware, las particiones de sistemas operativos y los datos asociados.

Nota Para asegurarse de no perder datos, mígrelos a otro equipo antes de instalar ESXi.

Si va a instalar ESXi en un disco que contiene una instalación anterior de ESXi o ESX, o bien un almacén de datos de VMFS, el instalador le brindará opciones para actualización. Consulte la documentación sobre la *actualización de vSphere*.

Instalar ESXi de manera interactiva

El servidor se arranca desde un CD o DVD de vSphere ESXi asociado, desde un dispositivo USB de arranque o mediante un arranque con PXE del servidor desde una ubicación de la red. Debe seguir las indicaciones del asistente de instalación para instalar ESXi en el disco.

Instalar ESXi de forma interactiva

Utilice el CD/DVD o una unidad flash USB de ESXi para instalar el software ESXi en un disco duro SAS, SATA o SCSI, o bien en una unidad USB.

Requisitos previos

- Debe tener el archivo ISO del instalador de ESXi en una de las siguientes ubicaciones:
  - Un CD o DVD. Si no posee el CD/DVD de instalación, puede crear uno. Consulte Descargar y grabar un CD or DVD de la imagen ISO del instalador de ESXi
  - Una unidad flash USB. Consulte Formatear una unidad flash USB para arrancar la instalación o la actualización de ESXi.

  Nota También puede realizar un arranque PXE del instalador de ESXi para ejecutar una instalación interactiva o por script. Consulte Arranque de red del instalador de ESXi.
- Compruebe que el reloj de hardware del servidor esté configurado como UTC. Este ajuste se encuentra en el BIOS o la UEFI del sistema.
- Compruebe que haya un teclado y un monitor conectados al equipo en el que está instalado el software ESXi. Como alternativa, utilice una aplicación de administración remota. Consulte Usar aplicaciones de administración remota.
- Considere la posibilidad de desconectar el almacenamiento de red. Esta acción disminuye el tiempo que tarda el instalador en buscar unidades de disco disponibles. Al desconectar el almacenamiento de red, ninguno de los archivos almacenados en los discos desconectados está disponible durante la instalación.

No desconecte un LUN que contenga una instalación de ESX o ESXi. No desconecte un almacén de datos de VMFS que contenga una consola de servicios de una instalación de ESX existente. Estas acciones podrían afectar el resultado de la instalación.

- Recopile la información que necesita el asistente de instalación de ESXi. Consulte Información obligatoria para instalar ESXi.
- Compruebe que ESXi Embedded no esté presente en el equipo host. ESXi Installable y ESXi Embedded no pueden estar en el mismo host.

Procedimiento

1 Inserte el CD/DVD del instalador de ESXi en la unidad de CD/DVD-ROM, o bien conecte la unidad flash USB del instalador, y reinicie el equipo.

2 Configure el BIOS o la UEFI para que arranque desde el dispositivo de CD-ROM o la unidad flash USB.

Nota Si el sistema tiene unidades de procesamiento de datos (DPU), solo puede usar UEFI para instalar y arrancar ESXi en las DPU.

Consulte la documentación del proveedor de hardware para obtener información sobre el cambio del orden de arranque.

3 En la pantalla de bienvenida, presione Intro para continuar.

4 Para aceptar el contrato de licencia de usuario final, presione **Intro**.

A partir de ESXi 8.0 Update 3, una vez finalizada la exploración de los dispositivos disponibles, si el sistema tiene varias DPU, estas aparecerán automáticamente con sus respectivas ranuras PCI. Ya no es necesario que seleccione una ranura. Los dispositivos DPU deben ser idénticos: el mismo proveedor, la misma versión de hardware y el mismo firmware.

5 En la página **Seleccionar un disco para instalar o actualizar ESXi**, seleccione la unidad en la que va a instalar ESXi y presione **Intro**.

Presione F1 para obtener más información sobre el disco seleccionado.

Nota No se base en el orden de discos de la lista para seleccionar un disco. El BIOS o la UEFI determinan el orden de los discos y podría estar desordenado. Esto puede ocurrir en sistemas en los que se agregan y eliminan unidades continuamente.

Si selecciona un disco que contiene datos, aparece la página **Confirmar selección de disco**.

Si va a realizar la instalación en un disco que tiene una instalación anterior de ESXi o ESX, o bien en un almacén de datos de VMFS, el instalador proporciona varias alternativas.

Importante Si va a actualizar o migrar una instalación de ESXi existente, consulte la documentación sobre *Actualizar VMware ESXi*.

Si selecciona un disco del grupo de discos de vSAN, la instalación que se obtenga dependerá del tipo de disco y del tamaño del grupo:

- Si selecciona una SSD, esta y todas las HDD subyacentes del mismo grupo de discos se borrarán.
- Si selecciona una HDD y el tamaño del grupo de discos es mayor que 2, solo se borrará la HDD seleccionada.
- Si selecciona una HDD y el tamaño del grupo de discos es 2 o menos, se borrarán la SSD y la HDD seleccionada.

6 Seleccione el tipo de teclado para el host.

Después de la instalación, puede cambiar el tipo de teclado en la consola directa.

7 Escriba la contraseña raíz para el host.

Después de la instalación, puede cambiar la contraseña en la consola directa.

8 En la pantalla **Confirmar instalación**, si el sistema vSphere tiene varias DPU, cada una de ellas aparecerá en una fila independiente. Pulse `F11` para confirmar el inicio de la instalación.

A partir de 8.0 Update 3, si los sistemas tienen varias DPU, verá una única barra de progreso para la instalación de ESXi y DPU, con actualizaciones dinámicas en la etiqueta que muestra qué etapa del instalador se está ejecutando.

Para obtener más información acerca de la administración de grupos de discos de vSAN, consulte la documentación de *Almacenamiento de vSphere*.

Si selecciona un dispositivo SD o USB, verá una advertencia que le solicita que seleccione un disco persistente para almacenar la partición ESXi-OSData. En la pantalla **Seleccione un disco para almacenar ESX OSData**, seleccione un dispositivo de almacenamiento persistente con un mínimo de 32 GB de espacio disponible.

9 Una vez que esta finaliza, quite el CD, el DVD o la unidad flash USB de instalación.

A partir de 8.0 Update 3, si la instalación no se realiza correctamente en alguno de los destinos, verá la pantalla **Error en la operación**. Registre el registro de errores en la pantalla para ayudar a solucionar los problemas.

10 Presione **Intro** para reiniciar el host.

11 Configure el dispositivo de primer arranque como la unidad en la que instaló ESXi en Paso 5.

Para obtener más información sobre cómo cambiar el orden de arranque, consulte la documentación del proveedor de hardware.

Nota Es posible que se necesiten pasos adicionales para configurar el dispositivo de arranque en sistemas UEFI. Consulte El host no arranca después de instalar ESXi en modo UEFI

Resultados

Una vez finalizada la instalación, puede migrar los datos de VMFS existentes al host ESXi.

Puede arrancar un único equipo desde cada imagen de ESXi. No se permite arrancar varios dispositivos desde una única imagen compartida de ESXi.

Pasos siguientes

Establezca la configuración básica de administración y red para ESXi. Consulte Después de instalar y configurar ESXi.

Instalar ESXi en un disco iSCSI de software

Al instalar ESXi en un disco iSCSI de software, debe configurar el nombre calificado iSCSI (IQN) de destino.

Durante el arranque del sistema, se realiza una prueba automática de encendido (POST) y se comienzan a iniciar los adaptadores en el orden especificado en el BIOS del sistema. Cuando el orden de arranque llega al adaptador de la tabla de firmware de arranque de iSCSI (iBFT), el adaptador intenta conectarse al destino, pero no arranca desde el destino. Consulte los requisitos previos.

Si la conexión con el destino de iSCSI se establece correctamente, el firmware de arranque de iSCSI guarda la configuración de arranque de iSCSI en iBFT. El próximo adaptador en arrancar debe ser el medio de instalación de ESXi, que puede ser una imagen ISO montada o un CD-ROM físico.

Requisitos previos

- Compruebe que el IQN de destino esté establecido en la configuración de parámetros de destino del BIOS de iBFT. Esta configuración se encuentra en la opción ROM de la tarjeta de interfaz de red (NIC) que se debe usar para el LUN de iSCSI. Consulte la documentación del proveedor de su sistema.
- Desactive la opción del adaptador de iBFT para arrancar en el destino iSCSI. Esta acción es necesaria para garantizar el arranque del instalador de ESXi, en lugar del destino de iSCSI. Al iniciar el sistema, siga el aviso para iniciar sesión en el adaptador de iBFT y desactive la opción para arrancar en el destino de iSCSI. Consulte la documentación del proveedor de su sistema y su adaptador de iBFT. Después de finalizar la instalación de ESXi, puede volver a habilitar la opción para arrancar desde el LUN en el que instaló ESXi.

Procedimiento

1 Inicie la instalación interactiva desde la imagen ISO montada o el CD/DVD de instalación de ESXi.

2 En la pantalla Seleccionar un disco, seleccione el destino de iSCSI que especificó en la configuración de parámetros de destino del BIOS de iBFT.

   Si el destino no aparece en este menú, asegúrese de que la configuración de TCP/IP e IQN iSCSI del iniciador sea la correcta. Compruebe la lista de control de acceso (ACL) de la red y confirme que el adaptador cuenta con los permisos necesarios para acceder al destino.

3 Siga las indicaciones para completar la instalación.

4 Reinicie el host.

5 En la configuración del BIOS del host, especifique la configuración del BIOS para el adaptador de iBFT y cambie el parámetro del adaptador para que arranque desde el destino de iSCSI.

   Consulte la documentación del proveedor de su sistema.

Pasos siguientes

En el adaptador de iBFT, habilite nuevamente la opción para arrancar en el destino de iSCSI, de modo que el sistema arranque desde el LUN en el que instaló ESXi.

Instalar ESXi mediante un script

El script de instalación o actualización es un archivo de texto que contiene los comandos compatibles (por ejemplo, `ks.cfg`).

La sección de comandos del script contiene las opciones de instalación de ESXi. Esta sección es obligatoria y debe aparecer primero en el script.

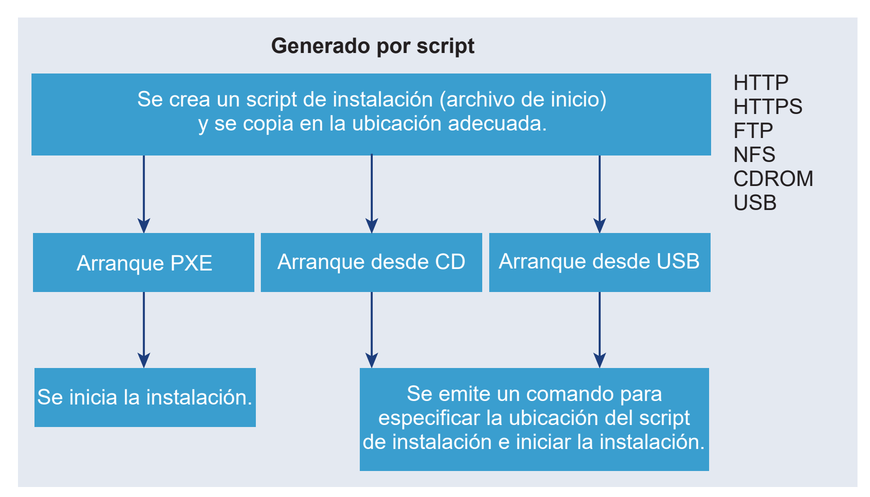
Instalación de ESXi generada por script

La ejecución de un script es una manera eficaz de implementar varios hosts ESXi mediante una instalación desatendida.

El script de instalación contiene los ajustes de configuración del host. Puede usar el script para configurar varios hosts con las mismas opciones. Consulte Instalar o actualizar hosts mediante un script.

El script de instalación debe almacenarse en una ubicación a la que el host pueda acceder mediante HTTP, HTTPS, FTP, NFS, CD-ROM o USB. Puede arrancar el instalador de ESXi mediante PXE o desde una unidad USB o de CD/DVD.

Figura 4-3. Instalación generada por script



Enfoques para la instalación por script

Puede instalar ESXi en varios equipos con un único script para todos o un script separado para cada uno.

Por ejemplo, debido a que los nombres de disco varían de un equipo a otro, una de las opciones de configuración que se recomienda seleccionar en un script es el disco en el que se va a instalar ESXi.

Tabla 4-12. Opciones de una instalación por script

Opción	Acción
Instalar siempre en el primer disco de varios equipos.	Crear un solo script.
Instalar ESXi en un disco distinto para cada equipo.	Crear varios scripts.

Para obtener información sobre los comandos necesarios para especificar el disco en el que se va a realizar la instalación, consulte Comandos de scripts de instalación y actualización.

Introducir las opciones de arranque para ejecutar un script de instalación o actualización

Puede iniciar un script de instalación o actualización introduciendo las opciones de arranque en la línea de comandos de arranque del instalador de ESXi.

En el momento del arranque, es posible que necesite especificar opciones para acceder al archivo de inicio. Puede introducir opciones de arranque presionando Shift+O en el gestor de arranque. Para una instalación de arranque PXE, puede pasar opciones a través de la línea `kernelopts` del archivo `boot.cfg`. Consulte Acerca del archivo boot.cfg y Arranque de red del instalador de ESXi.

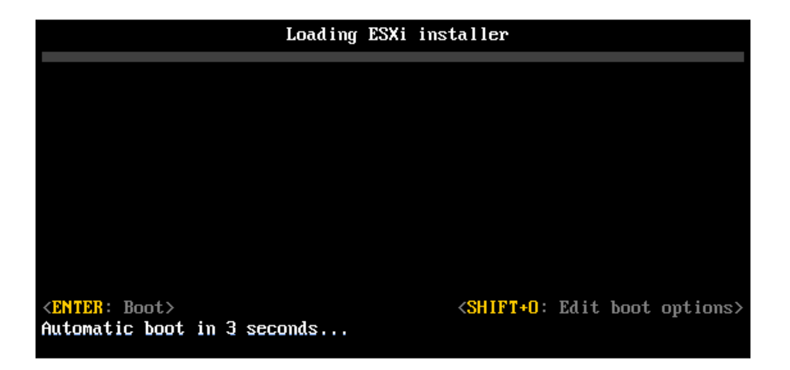
Para especificar la ubicación del script de instalación, defina la opción `ks=`*`filepath`*, donde *filepath* indica la ubicación del archivo Kickstart. De lo contrario, no se podrá iniciar una instalación o actualización generadas por script. Si se omite `ks=`*`filepath`*, se ejecuta el instalador de texto.

Las opciones de arranque compatibles se detallan en Opciones de arranque .

Procedimiento

1 Inicie el host.

2 Cuando aparezca la ventana del instalador de ESXi, presione las teclas Mayús + O para editar las opciones de arranque.



3 En el símbolo del sistema `runweasel`, introduzca **`ks=`*`ubicación del script de instalación más las opciones de la línea de comandos de arranque`***.

Ejemplo: Opción de arranque

Introduzca las siguientes opciones de arranque:

```
ks=http://00.00.00.00/kickstart/ks-osdc-pdp101.cfg nameserver=00.00.0.0 ip=00.00.00.000
netmask=255.255.255.0 gateway=00.00.00.000
```

Opciones de arranque

Cuando realice una instalación por script, es posible que necesite especificar opciones en el arranque para acceder al archivo de inicio.

Opciones de arranque compatibles

Tabla 4-13. Opciones de arranque para la instalación de ESXi

Opción de arranque	Descripción
`BOOTIF=`*`hwtype-MAC address`*	Similar a la opción `netdevice`, excepto en el formato PXELINUX, tal como se describe en la opción IPAPPEND en SYSLINUX en el sitio `syslinux.org`.
`gateway=`*`ip address`*	Permite establecer esta puerta de enlace de red como la puerta de enlace predeterminada para utilizarla en la descarga de scripts de instalación y medios de instalación.
`ip=`*`ip address`*	Permite configurar una dirección IP estática para utilizarla en la descarga de scripts de instalación y medios de instalación. Nota: también se admite el formato PXELINUX para esta opción. Consulte la opción IPAPPEND en SYSLINUX en el sitio `syslinux.org`.

Tabla 4-13. Opciones de arranque para la instalación de ESXi (continuación)

Opción de arranque	Descripción
`ks=cdrom:/path`	Permite realizar una instalación por script con el script en *path*, que se encuentra en el CD de la unidad de CD-ROM. Cada CDROM se monta y se comprueba hasta que se encuentre el archivo que coincida con la ruta de acceso. **Importante** Si creó una imagen ISO de instalador con un script de instalación o actualización personalizado, debe utilizar caracteres en mayúscula para proporcionar la ruta de acceso del script, por ejemplo, `ks=cdrom:/KS_CUST.CFG`.
`ks=file://path`	Realiza una instalación por script con el script en *path*.
`ks=protocol://serverpath`	Realiza una instalación por script con un script ubicado en la red en la dirección URL determinada. El *protocolo* puede ser `http`, `https`, `ftp` o `nfs`. Un ejemplo de uso del protocolo NFS es `ks=nfs://host/porturl-path`. El formato de la URL de NFS se especifica en RFC 2224.
`ks=usb`	Realiza una instalación por script mediante el acceso al script desde la unidad USB conectada. Busca un archivo con el nombre `ks.cfg`. El archivo debe estar ubicado en el directorio raíz de la unidad. Si se conectan varias unidades flash USB, se realizará la búsqueda hasta que se encuentre el archivo `ks.cfg`. Solo se admiten los sistemas de archivos FAT16 y FAT32.
`ks=usb:/path`	Realiza una instalación por script con un archivo de script en la ruta especificada, que se encuentra en USB.
`ksdevice=device`	Intenta utilizar un adaptador de red *device* cuando se realiza la búsqueda de un script de instalación y un medio de instalación. Se especifica como una dirección MAC, por ejemplo, 00:50:56:C0:00:01. Esta ubicación también puede ser un nombre vmnicNN. Si no se especifica y los archivos deben obtenerse a través de la red, el instalador utiliza de forma predeterminada el primer adaptador de red detectado que esté conectado.
`nameserver=ip address`	Especifica un servidor de nombres de dominio para utilizarlo en la descarga de scripts de instalación y medios de instalación.
`netdevice=device`	Intenta utilizar un adaptador de red *device* cuando se realiza la búsqueda de un script de instalación y un medio de instalación. Se especifica como una dirección MAC, por ejemplo, 00:50:56:C0:00:01. Esta ubicación también puede ser un nombre vmnicNN. Si no se especifica y los archivos deben obtenerse a través de la red, el instalador utiliza de forma predeterminada el primer adaptador de red detectado que esté conectado.
`netmask=subnet mask`	Especifica una máscara de subred para la interfaz de red que descarga los scripts de instalación y los medios de instalación.

Tabla 4-13. Opciones de arranque para la instalación de ESXi (continuación)

Opción de arranque	Descripción
`vlanid=`*`vlanid`*	Configure la tarjeta de red para que se encuentre en la VLAN especificada.
`systemMediaSize=`*`small`*	Limita el tamaño de las particiones de almacenamiento del sistema en los medios de arranque. El valor seleccionado debe adecuarse al propósito del sistema. Se puede elegir alguno de los siguientes valores: ■ *min* (32 GB, para servidores integrados o con un único disco) ■ *small* (64 GB, para servidores con al menos 512 GB de RAM) ■ *default* (128 GB) ■ *max* (consumir todo el espacio disponible, para servidores de varios terabytes)

Para más información sobre las opciones de inicio de ESXi posteriores a la instalación, consulte el artículo 77009 de la base de conocimientos de VMware.

Scripts de instalación y actualización utilizados para la instalación de ESXi

Puede utilizar un script predeterminado para realizar una instalación estándar ESXi en el primer disco detectado.

Durante una instalación de ESXi, puede usar un script predeterminado para realizar una instalación estándar en el primer disco detectado y el archivo de configuración del cargador de arranque para especificar el kernel, las opciones de kernel y los módulos de arranque que utiliza el cargador de arranque mboot.c32 o mboot.efi para la instalación.

Acerca del script de instalación predeterminado ks.cfg

El instalador de ESXi incluye un script de instalación predeterminado que realiza una instalación estándar en el primer disco detectado.

El script de instalación `ks.cfg` predeterminado está ubicado en el disco RAM inicial en `/etc/vmware/weasel/ks.cfg`. Puede especificar la ubicación del archivo `ks.cfg` predeterminado con la opción de arranque `ks=file://etc/vmware/weasel/ks.cfg`. Consulte Introducir las opciones de arranque para ejecutar un script de instalación o actualización.

Cuando instale ESXi con el script `ks.cfg`, la contraseña raíz predeterminada será `myp@ssw0rd`.

No puede modificar el script predeterminado en los medios de instalación. Después de la instalación, puede utilizar vSphere Client para iniciar sesión en vCenter Server que administra el host ESXi y modificar la configuración predeterminada.

Con vSphere 8.0, si el sistema tiene unidades de procesamiento de datos (Data Processing Units, DPU), se utiliza el script `ks.cfg` también para instalar ESXi en las DPU.

El script predeterminado contiene los siguientes comandos:

```
#
# Sample scripted installation file
#

# Accept the VMware End User License Agreement
vmaccepteula

# Set the root password for the DCUI and Tech Support Mode
rootpw myp@ssw0rd

# Install on the first local disk available on machine
install --firstdisk --overwritevmfs
 In case you system has DPUs, you also specify a PCI slot:
install --firstdisk --overwritevmfs --dpupcislots=<PCIeSlotID>

# Set the network to DHCP on the first network adapter
network --bootproto=dhcp --device=vmnic0

# A sample post-install script
%post --interpreter=python --ignorefailure=true
import time
stampFile = open('/finished.stamp', mode='w')
stampFile.write( time.asctime() )
```

Acerca del archivo boot.cfg

El archivo de configuración del cargador de arranque `boot.cfg` especifica el kernel, las opciones del kernel y los módulos de arranque que utiliza el cargador de arranque `mboot.c32` o `mboot.efi` en una instalación de ESXi.

El archivo `boot.cfg` se incluye en el instalador de ESXi. Puede modificar la línea `kernelopt` del archivo `boot.cfg` para especificar la ubicación de un script de instalación o para pasar otras opciones de arranque.

El archivo `boot.cfg` tiene la siguiente sintaxis:

```
# boot.cfg -- mboot configuration file
#
# Any line preceded with '#' is a comment.

title=STRING
prefix=DIRPATH
kernel=FILEPATH
kernelopt=STRING
modules=FILEPATH1 --- FILEPATH2... --- FILEPATHn

# Any other line must remain unchanged.
```

Los comandos de `boot.cfg` configuran el cargador de arranque.

Tabla 4-14. Comandos de `boot.cfg`.

Comando	Descripción
`title=STRING`	Establece el título del cargador de arranque como *STRING*.
`prefix=STRING`	(Opcional) Agrega *DIRPATH/* frente a cada *FILEPATH* en los comandos `kernel=` y `modules=` que no empiezan con / o con `http://`.
`kernel=FILEPATH`	Establece la ruta de acceso del kernel como *FILEPATH*.
`kernelopt=STRING`	Anexa *STRING* a las opciones de arranque del kernel.
`modules=FILEPATH1 --- FILEPATH2... --- FILEPATHn`	Enumera los módulos que se van a cargar, separados por tres guiones (`---`).

Consulte Crear una imagen ISO de instalador con un script de instalación o actualización personalizado y Arranque de red del instalador de ESXi.

Ubicaciones admitidas para scripts de instalación o actualización

En instalaciones y actualizaciones generadas por script, el instalador de ESXi puede acceder al script de la instalación o actualización, que también se conoce como el archivo inicial, desde varias ubicaciones.

Se admiten las siguientes ubicaciones para el script de instalación o actualización:

- CD/DVD. Consulte Crear una imagen ISO de instalador con un script de instalación o actualización personalizado.
- Unidad flash USB. Consulte Crear una unidad flash USB para almacenar el script de instalación o actualización de ESXi.
- Una ubicación local de red a la que se puede acceder mediante los siguientes protocolos: NFS, HTTP, HTTPS, FTP

Ruta de acceso del script de instalación o actualización

Puede especificar la ruta de acceso de un script de instalación o actualización.

`ks=http://XXX.XXX.XXX.XXX/kickstart/KS.CFG` es la ruta de acceso del script de instalación de ESXi, donde*XXX.XXX.XXX.XXX*es la dirección IP del equipo donde reside el script. Consulte Instalar ESXi mediante un script.

Para iniciar un script de instalación desde una instalación interactiva, escriba la opción `ks=` de forma manual. Consulte Introducir las opciones de arranque para ejecutar un script de instalación o actualización.

Comandos de scripts de instalación y actualización

Para modificar el script predeterminado de instalación o actualización, o para crear su propio script, use comandos compatibles. Use comandos compatibles en el script de instalación, que se especifica mediante un comando de arranque cuando se arranca el instalador.

Para determinar en qué disco instalar o actualizar ESXi, el script de instalación requiere uno de los comandos siguientes: install, upgrade o installorupgrade. El comando install crea las particiones predeterminadas, que incluyen un almacén de datos de VMFS que ocupa todo el espacio disponible después de que se crean las demás particiones.

Con vSphere 8.0, si el sistema tiene unidades de procesamiento de datos (DPU) admitidas, considere siempre la posibilidad de instalación, reinstalación o actualización de ESXi en las DPU además de ESXi en los hosts. La actualización de ESXi y la actualización en las DPU no es compatible con el método interactivo o con scripts, solo se puede usar vSphere Lifecycle Manager.

Nota El uso de dispositivos SD y USB para almacenar particiones de ESX-OSData está cayendo es desuso. Puede usar dispositivos SD y USB solo para crear particiones de banco de arranque, boot-bank 0 y boot-bank 1. También puede proporcionar un disco persistente de 32 GB como mínimo para instalar la partición ESX-OSData. Para definir estos discos, utilice el parámetro systemDisk en el comando install.

accepteula o vmaccepteula (obligatorio)

Acepta el contrato de licencia de ESXi.

clearpart (opcional)

Borra las particiones existentes del disco. Requiere que se especifique el comando install. Edite cuidadosamente el comando clearpart en sus scripts existentes.

--drives=	Quita las particiones en las unidades especificadas.
--alldrives	Ignora el requisito de --drives= y permite borrar las particiones de cada unidad.
--ignoredrives=	Elimina las particiones en todas las unidades, excepto las especificadas. Es obligatorio a menos que se especifiquen las marcas --drives= o --alldrives.
--overwritevmfs	Permite sobrescribir las particiones de VMFS en las unidades especificadas. De forma predeterminada, no se permite sobrescribir las particiones de VMFS.
--firstdisk= ***tipo-disco1*** **[*tipo-disco2*,...]**	**Nota** Si la versión del sistema vSphere es anterior a la 8.0 Update 3 y tiene DPU, también debe especificar una ranura PCI: install --firstdisk --overwritevmfs --dpupcislots=<PCIeSlotID>. Para los sistemas con la versión 8.0 Update 3 y posteriores, el parámetro dpupcislots ha quedado obsoleto.

Particiona el primer disco encontrado que satisface las condiciones. De forma predeterminada, los discos que satisfacen las condiciones se ordenan en el orden siguiente:

1 Almacenamiento conectado a nivel local (`local`)

2 Almacenamiento en red (`remote`)

Puede cambiar el orden de los discos anexando una lista separada por comas al argumento. Si proporciona una lista de filtros, se sobrescribe la configuración predeterminada. Puede combinar filtros para especificar un disco en particular, lo que incluye `esx` para el primer disco en el que se haya instalado ESXi, la información de modelo y proveedor, o el nombre del controlador del dispositivo VMkernel. Por ejemplo, para dar preferencia a un disco con el nombre de modelo ST3120814A y a cualquier disco que use el controlador mptsas en lugar de un disco local normal, el argumento es `--firstdisk=ST3120814A,mptsas,local`. Puede utilizar `localesx` para el almacenamiento local que contiene la imagen de ESXi o `remoteesx` para el almacenamiento remoto que contiene la imagen deESXi.

dryrun (opcional)

Analiza y comprueba el script de instalación. No ejecuta la instalación.

instalar

Especifica que se trata de una instalación nueva. Se requieren los comandos `install`, `upgrade` o `installorupgrade` para determinar en qué disco se debe instalar o actualizar ESXi.

`--disk= or --drive=`

Especifica el disco que se particionará. En el comando `--disk=`*`diskname`*, *diskname* puede ser un nombre de disco o una ruta completa de sistema de archivos de disco en ESXi, por ejemplo:

- Nombre de disco: `--disk=naa.6d09466044143600247aee55ca2a6405` o
- Ruta de acceso del dispositivo: `--disk=`*`/vmfs/devices/disks/mpx.vmhba1:C0:T0:L0`*

Para conocer los formatos admitidos de nombre de disco, consulte Nombre de los dispositivos de disco.

--firstdisk=

tipo-disco1,

[*tipo-disco2*,...]

Nota Si la versión del sistema vSphere es anterior a la 8.0 Update 3 y tiene DPU, también debe especificar una ranura PCI: install --firstdisk --overwritevmfs --dpupcislots=<PCIeSlotID>. Para los sistemas con la versión 8.0 Update 3 y posteriores, el parámetro dpupcislots ha quedado obsoleto.

Particiona el primer disco encontrado que satisface las condiciones. De forma predeterminada, los discos que satisfacen las condiciones se ordenan en el orden siguiente:

1 Almacenamiento conectado a nivel local (local)

2 Almacenamiento en red (remote)

Puede cambiar el orden de los discos anexando una lista separada por comas al argumento. Si proporciona una lista de filtros, se sobrescribe la configuración predeterminada. Puede combinar filtros para especificar un disco en particular, lo que incluye esx para el primer disco en el que se haya instalado ESX, la información de modelo y proveedor, o el nombre del controlador del dispositivo VMkernel. Por ejemplo, para dar preferencia a un disco con el nombre de modelo ST3120814A y a cualquier disco que use el controlador mptsas en lugar de un disco local normal, el argumento es --firstdisk=ST3120814A,mptsas,local. Puede utilizar localesx para el almacenamiento local que contiene la imagen de ESXi o remoteesx para el almacenamiento remoto que contiene la imagen deESXi.

--ignoressd

Excluye los discos de estado sólido de los que satisfacen las condiciones para el particionamiento. Esta opción puede utilizarse con el comando install y la opción --firstdisk. Esta opción tiene prioridad sobre la opción --firstdisk. Esta opción no es válida con las opciones --drive o --disk ni con los comandos upgrade o installorupgrade. Consulte la documentación de *Almacenamiento de vSphere* para obtener más información sobre la prevención del formateo de SSD durante la creación automática de particiones.

--overwritevsan

Debe usar la opción --overwritevsan cuando instale ESXi en un disco, ya sea SSD o HDD (magnética), que forme parte de un grupo de discos de vSAN. Si usa esta opción y no hay ninguna partición de vSAN en el disco seleccionado, se produce un error en la instalación.

Al instalar ESXi en un disco que forma parte de un grupo de discos de vSAN, el resultado depende del disco que se selecciona:

- Si selecciona una SSD, esta y todas las HDD subyacentes del mismo grupo de discos se borrarán.
- Si selecciona una HDD y el tamaño del grupo de discos es mayor que 2, solo se borrará la HDD seleccionada.
- Si selecciona una HDD y el tamaño del grupo de discos es 2 o menos, se borrarán la SSD y la HDD seleccionada.

Para obtener más información acerca de la administración de grupos de discos de vSAN, consulte la documentación de *Almacenamiento de vSphere*.

--overwritevmfs

Es obligatorio para sobrescribir un almacén de datos existente de VMFS en el disco antes de la instalación.

--preservevmfs

Conserva el almacén de datos existente de VMFS en el disco durante la instalación.

--novmfsondisk

Impide que se cree una partición de VMFS en este disco. Debe utilizarse con `--overwritevmfs` si existe una partición de VMFS en el disco.

--systemdisk

Si utiliza un dispositivo USB o SD, `systemDisk` especifica el disco persistente local en el que se instalará la partición ESX-OSData. Por ejemplo, **install --firstdisk = usb --systemDisk=<diskID>**. Como resultado, las particiones de banco de arranque se colocan en el dispositivo USB, mientras que la partición de OSData se encuentra en el disco especificado en el parámetro `systemDisk`.

--repartitionsystemdisk

Si utiliza un dispositivo USB o SD y el disco local que especificó con el parámetro `systemDisk` no está vacío o contiene un almacén de datos, puede usar `repartitionSystemDisk` para asegurarse de que el disco persistente se vuelva a particionar antes de usarlo.

Nota Si un disco persistente local no está disponible o el tamaño del disco es inferior a 32 GB, verá mensajes de advertencia, pero la instalación continúa.

--forceunsupportedinstall

Bloquea la instalación de CPU obsoletas.

installorupgrade

Se requieren los comandos `install`, `upgrade` o `installorupgrade` para determinar en qué disco se debe instalar o actualizar ESXi.

`--disk= or --drive=`

Especifica el disco que se particionará. En el comando `--disk=`*`diskname`*, *diskname* puede ser un nombre de disco o una ruta completa de sistema de archivos de disco en ESXi, por ejemplo:

- Nombre de disco: `--disk=naa.6d09466044143600247aee55ca2a6405` o
- Ruta de acceso del dispositivo: `--disk=`*`/vmfs/devices/disks/mpx.vmhba1:C0:T0:L0`*

Para conocer los formatos admitidos de nombre de disco, consulte Nombre de los dispositivos de disco.

`--firstdisk=`

`tipo-disco1,`

`[`*`tipo-disco2`*`,...]`

Nota Si la versión del sistema vSphere es anterior a la 8.0 Update 3 y tiene DPU, también debe especificar una ranura PCI: `install --firstdisk --overwritevmfs --dpupcislots=<PCIeSlotID>`. Para los sistemas con la versión 8.0 Update 3 y posteriores, el parámetro `dpupcislots` ha quedado obsoleto.

Particiona el primer disco encontrado que satisface las condiciones. De forma predeterminada, los discos que satisfacen las condiciones se ordenan en el orden siguiente:

1. Almacenamiento conectado a nivel local (`local`)
2. Almacenamiento en red (`remote`)

Puede cambiar el orden de los discos anexando una lista separada por comas al argumento. Si proporciona una lista de filtros, se sobrescribe la configuración predeterminada. Puede combinar filtros para especificar un disco en particular, lo que incluye `esx` para el primer disco en el que se haya instalado ESX, la información de modelo y proveedor, o el nombre del controlador del dispositivo VMkernel. Por ejemplo, para dar preferencia a un disco con el nombre de modelo ST3120814A y a cualquier disco que use el controlador mptsas en lugar de un disco local normal, el argumento es `--firstdisk=ST3120814A,mptsas,local`. Puede utilizar `localesx` para el almacenamiento local que contiene la imagen de ESXi o `remoteesx` para el almacenamiento remoto que contiene la imagen deESXi.

`--overwritevsan`

Debe usar la opción `--overwritevsan` cuando instale ESXi en un disco, ya sea SSD o HDD (magnética), que forme parte de un grupo de discos de vSAN. Si usa esta opción y no hay ninguna partición de

vSAN en el disco seleccionado, se produce un error en la instalación. Al instalar ESXi en un disco que forma parte de un grupo de discos de vSAN, el resultado depende del disco que se selecciona:

- Si selecciona una SSD, esta y todas las HDD subyacentes del mismo grupo de discos se borrarán.
- Si selecciona una HDD y el tamaño del grupo de discos es mayor que 2, solo se borrará la HDD seleccionada.
- Si selecciona una HDD y el tamaño del grupo de discos es 2 o menos, se borrarán la SSD y la HDD seleccionada.

Para obtener más información acerca de la administración de grupos de discos de vSAN, consulte la documentación de *Almacenamiento de vSphere*.

`--overwritevmfs`

Instale ESXi si en el disco existe una partición de VMFS, pero no una instalación de ESX ni ESXi. A menos que esta opción esté presente, se producirá un error en el instalador si en el disco existe una partición de VMFS, pero no una instalación de ESX o de ESXi.

keyboard (opcional)

Configura el tipo de teclado para el sistema.

`keyboardType`

Especifica el mapa del teclado para el tipo de teclado seleccionado. *keyboardType* debe ser uno de los siguientes tipos.

- Belgian
- Brazilian
- Croatian
- Czechoslovakian
- Danish
- Estonian
- Finnish
- Francés
- Alemán
- Greek
- Icelandic
- Italian
- Japonés
- Latin American

- Norwegian
- Polish
- Portuguese
- Russian
- Slovenian
- Español
- Swedish
- Swiss French
- Swiss German
- Turkish
- Ukrainian
- United Kingdom
- Inglés americano (predeterminado)
- US Dvorak

serialnum o vmserialnum (opcional)

El comando se admite en ESXi 5.1 y versiones posteriores. Configura las licencias. Si no se incluye, ESXi se instala en modo de evaluación.

--esx=<license-key>	Especifica la clave de licencia de vSphere que se utilizará. El formato corresponde a cinco grupos de cinco caracteres (XXXXX-XXXXX-XXXXX-XXXXX-XXXXX).

network (opcional)

Especifica una dirección de red para el sistema.

--bootproto=[dhcp|static]	Especifica si la configuración de red se debe obtener desde DHCP o si se debe configurar de forma manual.
--device=	Especifica la dirección MAC de la tarjeta de red o el nombre del dispositivo, con el formato `vmnicNN` (por ejemplo, `vmnic0`). Esta opción hace referencia al dispositivo del vínculo superior para el conmutador virtual.
--ip=	Establece una dirección IP para el equipo que se va a instalar, con el formato `xxx.xxx.xxx.xxx`. Es obligatorio cuando se usa la opción `--bootproto=static` y se ignora en los demás casos.

--gateway=
: Designa la puerta de enlace predeterminada como una dirección IP, con el formato `xxx.xxx.xxx.xxx`. Se usa con la opción `--bootproto=static`.

--nameserver=
: Designa el servidor de nombre principal como una dirección IP. Se usa con la opción `--bootproto=static`. Omita esta opción si no va a usar DNS.

  La opción `--nameserver` puede admitir dos direcciones IP. Por ejemplo: `--nameserver="10.126.87.104[,10.126.87.120]"`

--netmask=
: Especifica la máscara de subred para el sistema instalado, con el formato `255.xxx.xxx.xxx`. Se usa con la opción `--bootproto=static`.

--hostname=
: Especifica el nombre de host para el sistema instalado.

--vlanid= *vlanid*
: Especifica la VLAN en la que reside el sistema. Se usa con las opciones `--bootproto=dhcp` o `--bootproto=static`. Se establece como un valor entero entre 1 y 4096.

--addvmportgroup=(0|1)
: Especifica si se debe agregar el grupo de puertos de la red de máquinas virtuales (VM), que utilizan las máquinas virtuales. El valor predeterminado es 1.

paranoid (opcional)

Hace que los mensajes de advertencia interrumpan la instalación. Si omite este comando, los mensajes de advertencia se registran.

part o partition (opcional)

Crea un almacén de datos de VMFS en el sistema. Solo se puede crear un almacén de datos por cada disco. No se puede usar en el mismo disco que el comando `install`. Solo se puede especificar una partición por cada disco y solo puede ser una partición de VMFS.

datastore name
: Especifica dónde se debe montar la partición.

--ondisk= or --ondrive=
: Especifica el disco o la unidad en la que se crea la partición.

--onfirstdisk=

***tipo-disco1*, [*tipo-disco2*,...]**

Nota Si la versión del sistema vSphere es anterior a la 8.0 Update 3 y tiene DPU, también debe especificar una ranura PCI: install --firstdisk --overwritevmfs --dpupcislots=<PCIeSlotID>. Para los sistemas con la versión 8.0 Update 3 y posteriores, el parámetro dpupcislots ha quedado obsoleto.

Particiona el primer disco encontrado que satisface las condiciones. De forma predeterminada, los discos que satisfacen las condiciones se ordenan en el orden siguiente:

1 Almacenamiento conectado a nivel local (`local`)

2 Almacenamiento en red (`remote`)

Puede cambiar el orden de los discos anexando una lista separada por comas al argumento. Si proporciona una lista de filtros, se sobrescribe la configuración predeterminada. Puede combinar filtros para especificar un disco en particular, lo que incluye `esx` para el primer disco en el que se haya instalado ESX, la información de modelo y proveedor, o el nombre del controlador del dispositivo VMkernel. Por ejemplo, para dar preferencia a un disco con el nombre de modelo ST3120814A y a cualquier disco que use el controlador mptsas en lugar de un disco local normal, el argumento es `--onfirstdisk=ST3120814A,mptsas,local`. Puede utilizar `localesx` para el almacenamiento local que contiene la imagen de ESXi o `remoteesx` para el almacenamiento remoto que contiene la imagen deESXi.

reboot (opcional)

Reinicia la máquina después de que finaliza la instalación generada por script.

<--noeject>	No se expulsa el CD después de la instalación.

rootpw (obligatorio)

Configura la contraseña raíz para el sistema.

--iscrypted	Especifica que la contraseña está cifrada.
password	Especifica el valor de la contraseña.

actualizar

Se requieren los comandos `install`, `upgrade` o `installorupgrade` para determinar en qué disco se debe instalar o actualizar ESXi.

--disk= or --drive=	Especifica el disco que se particionará. En el comando `--disk=`*`diskname`*, *diskname* puede ser un nombre de disco o una ruta completa de sistema de archivos de disco en ESXi, por ejemplo: ■ Nombre de disco: `--disk=naa.6d09466044143600247aee55ca2a6405` o ■ Ruta de acceso del dispositivo: `--disk=`*`/vmfs/devices/disks/mpx.vmhba1:C0:T0:L0`*

	Para conocer los formatos admitidos de nombre de disco, consulte Nombre de los dispositivos de disco.
--firstdisk= ***tipo-disco1,*** **[*tipo-disco2*,...]**	Particiona el primer disco encontrado que satisface las condiciones. De forma predeterminada, los discos que satisfacen las condiciones se ordenan en el orden siguiente: 1 Almacenamiento conectado a nivel local (`local`) 2 Almacenamiento en red (`remote`) Puede cambiar el orden de los discos anexando una lista separada por comas al argumento. Si proporciona una lista de filtros, se sobrescribe la configuración predeterminada. Puede combinar filtros para especificar un disco en particular, lo que incluye `esx` para el primer disco en el que se haya instalado ESX, la información de modelo y proveedor, o el nombre del controlador del dispositivo VMkernel. Por ejemplo, para dar preferencia a un disco con el nombre de modelo ST3120814A y a cualquier disco que use el controlador mptsas en lugar de un disco local normal, el argumento es `--firstdisk=ST3120814A,mptsas,local`. Puede utilizar `localesx` para el almacenamiento local que contiene la imagen de ESXi o `remoteesx` para el almacenamiento remoto que contiene la imagen deESXi.

%include o include (opcional)

Especifica otro script de instalación para analizar. Este comando se utiliza de manera similar a un comando de varias líneas, pero usa solamente un argumento.

filename	Por ejemplo: `%include part.cfg`

%pre (opcional)

Especifica un script para ejecutar antes de que se evalúe la configuración de inicio. Por ejemplo, puede usarse para generar los archivos que incluirá el archivo de inicio.

--interpreter =[python|busybox]	Especifica el intérprete que se usará. El valor predeterminado es busybox.

%post (opcional)

Ejecuta el script especificado después de que finaliza la instalación del paquete. Si se especifican varias secciones `%post`, se ejecutan en el orden en que aparecen en el script de instalación.

--interpreter	Especifica el intérprete que se usará. El valor predeterminado es busybox.

`=[python|busybox]`	
`--timeout=secs`	Especifica el límite de tiempo de espera para la ejecución del script. Si el script no finalizó cuando se agota el tiempo de espera, el script se interrumpe de manera forzosa.
`--ignorefailure =[true|false]`	Si se configura como true, la instalación se considera correcta incluso si el script `%post` finalizó con un error.

%firstboot

Crea un script `init` que se ejecuta solamente durante el primer arranque. El script no afecta los arranques posteriores. Si se especifican varias secciones `%firstboot`, se ejecutan en el orden en que aparecen en el archivo de inicio.

Nota No es posible comprobar la semántica de los scripts `%firstboot` hasta el primer arranque del sistema. Un script `%firstboot` puede contener errores potencialmente catastróficos que no se detectan sino hasta después de la finalización de la instalación.

Importante El script `%firstboot` no se ejecuta si el arranque seguro está habilitado en el host ESXi.

`--interpreter =[python|busybox]`	Especifica el intérprete que se usará. El valor predeterminado es busybox.

Nota No es posible comprobar la semántica del script `%firstboot` hasta el primer arranque del sistema. Si el script contiene errores, no se detectan sino hasta después de la finalización de la instalación.

Nombre de los dispositivos de disco

Para los comandos del script de instalación `install`, `upgrade` e `installorupgrade`, es necesario usar los nombres de dispositivos de disco.

Tabla 4-15. Nombre de los dispositivos de disco

Formato	Ejemplo	Descripción
NAA	naa.6d09466044143600247aee55ca2a6405	Identificador SCSI INQUIRY
EUI	eui.3966623838646463	Identificador SCSI INQUIRY
T10	t10.SanDisk00Cruzer_Blade000000004C5300 01171118101244	Identificador SCSI INQUIRY
VML	vml.00025261	Identificador de VMkernel heredado
MPX	mpx.vmhba0:C0:T0:L0	Identificador basado en rutas

Para obtener más información sobre los nombres de dispositivos de almacenamiento, consulte *Identificadores y nombres de dispositivos de almacenamiento* en la documentación de *Almacenamiento de vSphere*.

Configurar orígenes externos durante la instalación generada por script

A partir de ESXi 8.0 Update 1, es posible configurar orígenes de entropía externos en el archivo de inicio de una instalación generada por script.

Puede configurar ESXi en un entorno de alta seguridad para consumir entropía de orígenes de entropía externos, como un módulo de seguridad de hardware (Hardware Security Module, HSM), y alinearse con estándares como BSI Common Criteria, EAL4 y NIST FIPS CMVP, mediante el método de instalación por script.

ESXi 8.0 Update 1 introduce un daemon de entropía, `entropyd`, que crea un endpoint de vAPI para proporcionar una REST API que consulte y envíe datos de entropía a hosts ESXi. El daemon de entropía tiene varios parámetros configurables: `in-memory-cache size`, `in-storage-cache size`, `in-memory-low watermark` y `entropy-lost-timeout`. Los orígenes de entropía, tanto internos como externos, se recopilan en el módulo de mezclador de entropía. El daemon de entropía reenvía los orígenes de entropía desde el mezclador al grupo de entropía del kernel.

Si no necesita seleccionar orígenes de entropía externos, no habrá que cambiar nada en los scripts actuales.

Solo se pueden configurar orígenes de entropía externos para instalaciones nuevas. El daemon de entropía utiliza datos de entropía transmitidos durante la instalación en el primer arranque.

Nota No se puede utilizar ningún otro método, como la instalación interactiva, una imagen de clúster o Auto Deploy, para configurar orígenes de entropía externos. No se puede habilitar la función en un host ESXi existente .

Antes de actualizar el archivo de inicio, debe obtener datos de entropía binarios legítimos a partir de un origen externo, como HSM y guardarlos como un archivo cuyo tamaño esté comprendido entre 512 KB y 10 MB; por ejemplo, `entropy_data.dat`. A continuación, debe codificar el contenido del archivo `entropy_data` en un formato base64 válido para crear otro archivo; por ejemplo, `entropy_data.b64`.

En el archivo de inicio, se proporcionan los siguientes parámetros nuevos como parte del comando `entropy`:

- `data`: los datos de entropía con codificación Base64 procedentes de un origen externo.

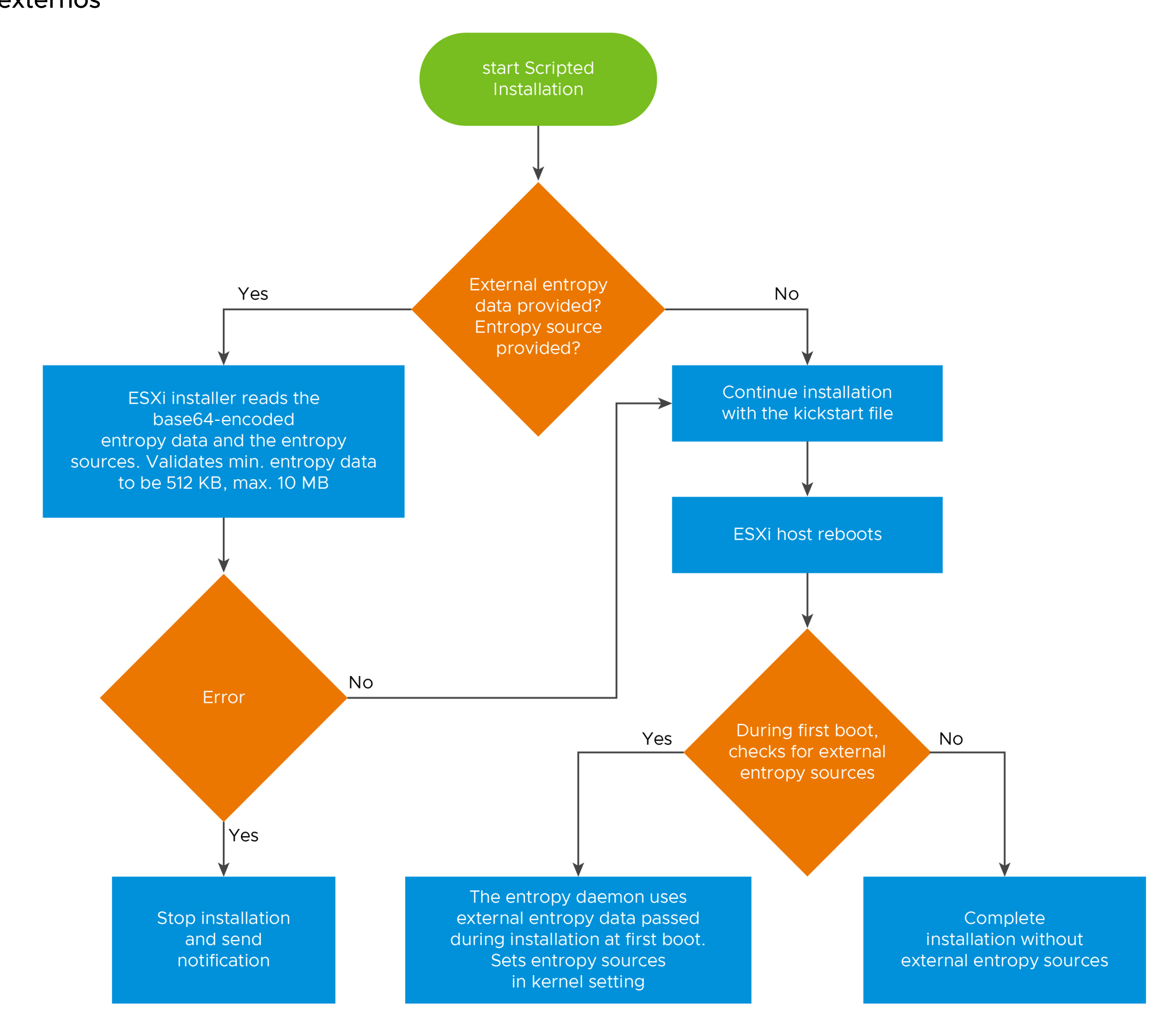
- 2: este valor de máscara de bits (=default 4, =interrupts 8, =RDRAND sources, 0=**RDSEED**, 1=**entropyd**). se establece en la configuración del kernel durante la instalación. Si se admite **RDSEED**, el valor predeterminado es la conformidad con FIPS. De lo contrario, el valor predeterminado son todos los orígenes de entropía, excepto **entropyd**. Para la conformidad de EAL4, 8 es el único valor necesario, pero se pueden utilizar otros orígenes del rango decimal 0–15. Los valores de origen se conservan como configuración de kernel durante la instalación.

  Nota Si configura un host ESXi solo con orígenes de entropía externa, es decir, cuando el valor de sources se establece en **8**, debe seguir proporcionando entropía externa al host mediante la API de entropía. Si se agota la entropía externa en el host, el host deja de responder y puede requerir un reinicio completo o una reinstalación para recuperarlo de dicha situación.

Un archivo de inicio de ejemplo con parámetros de entropía:

```
vmaccepteula
rootpw xxxxxxxx
entropy --sources=8 --data=xxxxxxx/xx/xxxxx/xx/xxxx...
install --firstdisk --overwritevmfs
network --bootproto=dhcp
```

Figura 4-4. Flujo de trabajo de instalación generado por script para agregar orígenes de entropía externos



Una vez que finalice la instalación, podrá iniciar sesión en el host ESXi y definir algunos parámetros para el daemon de entropía desde el shell mediante los siguientes comandos ESXCLI:

Comandos ESXCLI

1. Obtener comandos

##	esxcli system entropyd get	Descripción del comando
1	`<no argument>`	Obtenga los valores predeterminados y configurados actualmente de todos los parámetros de `entropyd`
2	`--default-values`	Obtener valores predeterminados

2. Establecer comandos

##	esxcli system entropyd set	Descripción del comando
1	--help	Imprima los detalles del comando "esxcli system entropyd set" y sus argumentos.
2	--reset=all --reset=memory-cache-size --reset=memory-cache-low-watermark --reset=storage-cache-size --reset=external-entropy-lost-timeout	Restablezca un parámetro o todos los parámetros a sus valores predeterminados .
3	--memory-cache-size=<value in KiB>	Establezca el tamaño de la memoria caché en KiB.
4	--memory-cache-low-watermark=<value in %>	Establezca la marca de agua baja de la memoria caché en porcentaje.
5	--storage-cache-size=<value in KiB>	Establezca el tamaño de la memoria caché de almacenamiento en KiB.
6	--external-entropy-lost-timeout=<value in seconds>	Establezca el tiempo de espera perdido de entropía externa en segundos.

Ejemplo:

```
$ esxcli system entropyd set --external-entropy-lost-timeout=70 --memory-cache-low-
watermark=30 --memory-cache-size=612 --storage-cache-size=5096
$ esxcli system entropyd get
External Entropy Lost Timeout Seconds: 70
Memory Cache Low Watermark Percentage: 30
Memory Cache Size Kibibytes: 612
Storage Cache Size Kibibytes: 5096

$ esxcli system entropyd get --default-values
External Entropy Lost Timeout Seconds: 60
Memory Cache Low Watermark Percentage: 20
Memory Cache Size Kibibytes: 512
Storage Cache Size Kibibytes: 4096
```

Durante la instalación, el instalador de ESXi actualiza el valor de los orígenes de entropía en la configuración del kernel para que persista en ConfigStore después de la instalación. Este cambio no afecta al arranque seguro de los hosts ESXi.

Para obtener más información, consulte las guías Seguridad de vSphere y Programación de vSphere Automation SDK.

Instalar o actualizar ESXi desde un CD o DVD con un script

Puede instalar o actualizar ESXi desde una unidad de CD-ROM o DVD-ROM utilizando un script que especifique las opciones de instalación o actualización.

Puede iniciar el script de instalación o actualización introduciendo una opción de arranque cuando inicie el host. También puede crear una imagen ISO de instalador que incluya el script de instalación. Puede utilizar una imagen ISO de instalador para realizar una instalación generada por script y desatendida cuando arranque con la imagen ISO de instalador resultante. Consulte Crear una imagen ISO de instalador con un script de instalación o actualización personalizado.

Requisitos previos

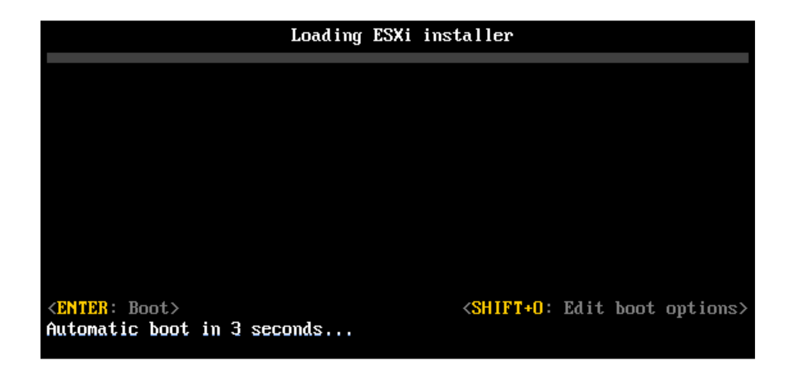
Antes de ejecutar la instalación o la actualización generadas por script, asegúrese de que se cumplen los siguientes requisitos previos:

- El sistema en el que va a realizar la instalación o actualización cumple con los requisitos de hardware. Consulte Requisitos de hardware de ESXi.
- Tiene el ISO con el instalador de ESXi en un CD o DVD de instalación. Consulte Descargar y grabar un CD or DVD de la imagen ISO del instalador de ESXi.
- El sistema puede acceder al script de instalación o actualización predeterminado (`ks.cfg`) o a un script de instalación o actualización personalizado. Consulte Instalar ESXi mediante un script.
- Ha seleccionado un comando de arranque para ejecutar la instalación o actualización generada por script. Consulte Introducir las opciones de arranque para ejecutar un script de instalación o actualización. Para obtener una lista completa de los comandos de arranque, consulte Opciones de arranque .

Procedimiento

1 Arranque el instalador de ESXi desde la unidad de CD-ROM o DVD-ROM local.

2 Cuando aparezca la ventana del instalador de ESXi, presione las teclas Mayús + O para editar las opciones de arranque.



3 Introduzca una opción de arranque que invoque al archivo de script de instalación o actualización predeterminado o uno que haya creado.

La opción de arranque tiene el formato `ks=`.

4 Presione Intro.

Resultados

Se ejecuta la operación de instalación, actualización o migración, utilizando las opciones que especificó.

Instalar o actualizar ESXi desde una unidad USB con un script

Puede instalar o actualizar ESXi desde una unidad flash USB utilizando un script que especifique las opciones de instalación o actualización.

Las opciones de arranque compatibles se detallan en Opciones de arranque .

Requisitos previos

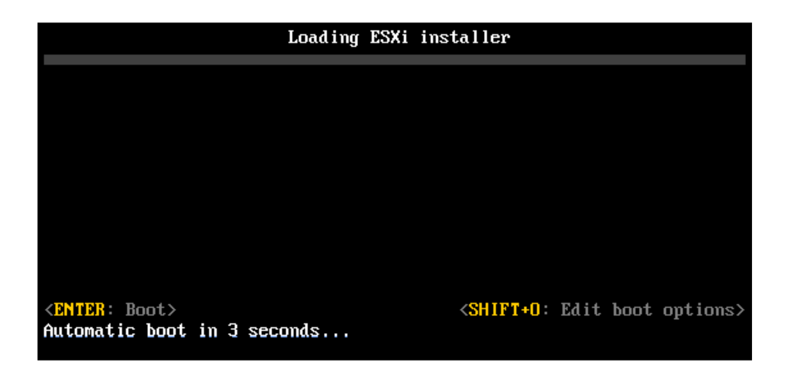
Antes de ejecutar la instalación o la actualización generadas por script, asegúrese de que se cumplen los siguientes requisitos previos:

- El sistema en el que va a realizar la instalación o la actualización a ESXi cumple con los requisitos de hardware para la instalación o la actualización. Consulte Requisitos de hardware de ESXi.
- Tiene el ISO con el instalador de ESXi en una unidad USB flash de arranque. Consulte Formatear una unidad flash USB para arrancar la instalación o la actualización de ESXi.
- El sistema puede acceder al script de instalación o actualización predeterminado (`ks.cfg`) o a un script de instalación o actualización personalizado. Consulte Instalar ESXi mediante un script.
- Ha seleccionado una opción de arranque para ejecutar la instalación, la actualización o la migración generadas por script. Consulte Introducir las opciones de arranque para ejecutar un script de instalación o actualización.

Procedimiento

1 Arranque el instalador de ESXi desde la unidad flash USB.

2 Cuando aparezca la ventana del instalador de ESXi, presione las teclas Mayús + O para editar las opciones de arranque.



3 Introduzca una opción de arranque que invoque al archivo de script de instalación o actualización predeterminado o uno que haya creado.

   La opción de arranque tiene el formato `ks=`.

4 Presione Intro.

Resultados

Se ejecuta la operación de instalación, actualización o migración, utilizando las opciones que especificó.

Arranque de red del instalador ESXi para una instalación o actualización generadas por script

ESXi 8.0 ofrece varias opciones para utilizar para arrancar el instalador en una red y utilizar un script de instalación o actualización.

- Para obtener información sobre la configuración de una infraestructura de red, consulte Arranque de red del instalador de ESXi.
- Para obtener información sobre la creación y ubicación de un script de instalación, consulte Instalar ESXi mediante un script.
- Para conocer procedimientos específicos para utilizar el arranque de red para arrancar el instalador de ESXi y utilizar un script de instalación, consulte uno de los siguientes temas:
  - Arrancar el instalador de ESXi mediante HTTP de UEFI nativo
  - Arrancar el instalador de ESXi mediante iPXE y HTTP
  - Arrancar el instalador de ESXi mediante PXE y TFTP
- Para obtener información sobre la utilización de vSphere Auto Deploy para realizar una instalación generada por script a través de PXE para arrancar, consulte Instalar ESXi con vSphere Auto Deploy .

Cómo arrancar un host ESXi desde un dispositivo de red

Arranque de red del instalador de ESXi

Puede utilizar el entorno de ejecución previo al arranque (PXE) para arrancar un host ESXi desde un dispositivo de red si el host utiliza el UEFI o BIOS heredado.

De forma alternativa, si el host ESXi es compatible con UEFI HTTP nativo, puede utilizar el protocolo de transferencia de hipertexto (HTTP) para arrancar el host desde un dispositivo de red. ESXi se distribuye en un formato ISO que se utiliza para instalarse en la memoria flash o en un disco duro local. Puede extraer los archivos y arrancarlos a través de una interfaz de red.

PXE utiliza el protocolo de configuración dinámica de host (DHCP) y el protocolo trivial de transferencia de archivos (TFTP) para arrancar un sistema operativo a través de una red.

El arranque con PXE requiere determinada infraestructura de red y una máquina con un adaptador de red compatible con PXE. La mayoría de las máquinas que pueden ejecutar ESXi poseen adaptadores de red que pueden arrancar con PXE.

El UEFI HTTP nativo utiliza DHCP y HTTP para arrancar a través de una red. El arranque UEFI HTTP requiere una infraestructura de red, una versión de firmware UEFI en el host de ESXi que incluye la función de arranque HTTP y un adaptador de red que admita redes UEFI.

El arranque mediante HTTP es más rápido y fiable que el uso de TFTP. Esto se debe a las capacidades del protocolo TCP subyacente a HTTP, como la transmisión integrada y la recuperación de paquetes perdidos. Si los hosts ESXi no son compatibles con el protocolo UEFI HTTP nativo, puede utilizar iPXE HTTP para el proceso de arranque.

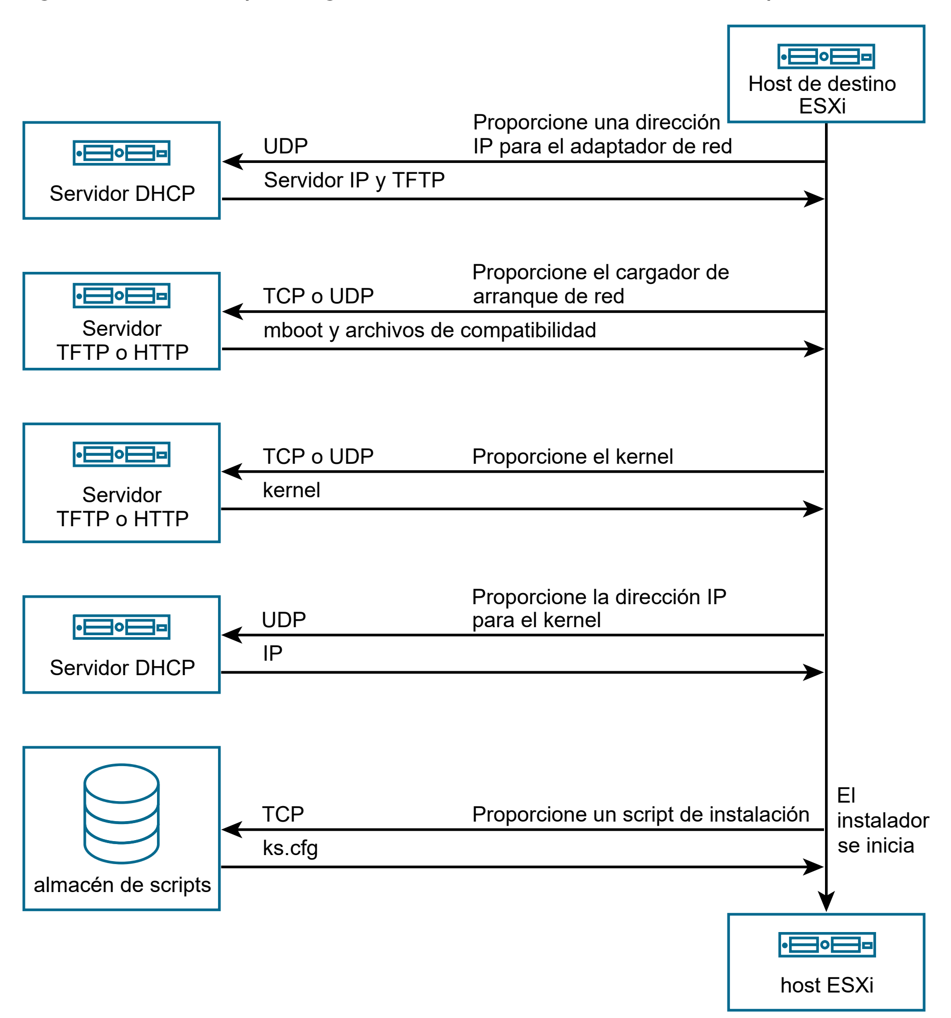
Nota El arranque de red con firmware de BIOS heredado solo se puede realizar mediante IPv4. El arranque de red con firmware de UEFI BIOS es posible a través de IPv4 o IPv6.

Descripción general de la instalación para el arranque de red

Puede arrancar un host ESXi desde una interfaz de red. Algunos de los detalles del proceso de arranque de red varían si el host de destino utiliza firmware de UEFI o BIOS heredado y si el proceso de arranque utiliza PXE TFTP, iPXE HTTP o UEFI HTTP.

Cuando se arranca un host de destino, este host interactúa con los diversos servidores en el entorno para obtener el adaptador de red, el cargador de arranque, el kernel, la dirección IP del kernel y, finalmente, un script de instalación. Una vez obtenidos todos los componentes, se inicia la instalación, como se muestra en la siguiente ilustración.

Figura 4-5. Descripción general de la instalación del arranque PXE



La interacción entre el host ESXi y los otros servidores continúa de la siguiente manera:

1 El usuario arranca el host ESXi de destino.

2 El host ESXi de destino realiza una solicitud DHCP.

3 El servidor DHCP responde con la información de IP, la ubicación del servidor TFTP o HTTP, y el nombre de archivo o la dirección URL del cargador de arranque de red inicial.

4 El host ESXi se pone contacto con el servidor TFTP o HTTP, y solicita el nombre de archivo o la URL que especificó el servidor DHCP.

5 El servidor TFTP o HTTP envía el cargador de arranque de red, y el host ESXi lo ejecuta. Es posible que el cargador de arranque inicial cargue componentes de cargador de arranque adicionales del servidor.

6 El cargador de arranque busca un archivo de configuración en el servidor TFTP o HTTP, descarga el kernel y otros componentes de ESXi según lo especificado en el archivo de configuración e inicia el kernel en el host ESXi.

7 El instalador se ejecuta de forma interactiva o mediante un script de inicio, según se especifique en el archivo de configuración.

Información sobre el arranque de red

Comprender el proceso de arranque de red puede ayudarle durante la solución de problemas.

Servidor TFTP

El protocolo trivial de transferencia de archivos (TFTP) es similar al servicio FTP y se utiliza generalmente solo para los sistemas de arranque de red o la carga de firmware en dispositivos de red, como los enrutadores. TFTP está disponible en Linux y Windows.

- La mayoría de las distribuciones de Linux incluyen una copia del servidor tftp-hpa. Si requiere una solución compatible, adquiera un servidor TFTP compatible de su proveedor de confianza. También puede adquirir un servidor TFTP desde uno de los dispositivos de paquete en VMware Marketplace.
- Si su servidor TFTP funciona en un host de Microsoft Windows, utilice tftpd32 versión 2.11 o una versión posterior. Consulte http://tftpd32.jounin.net/.

SYSLINUX y PXELINUX

Si utiliza PXE en un entorno BIOS heredado, debe comprender los distintos entornos de arranque.

- SYSLINUX es un entorno de arranque de código abierto para máquinas que ejecutan firmware de BIOS heredado. El cargador de arranque de ESXi para sistemas BIOS, `mboot.c32`, se ejecuta como un complemento de SYSLINUX. Puede configurar SYSLINUX para el arranque desde distintos tipos de medios, como un disco, una imagen ISO y una red. Puede encontrar el paquete de SYSLINUX en http://www.kernel.org/pub/linux/utils/boot/syslinux/.
- PXELINUX es una configuración de SYSXLINUX para realizar el arranque desde un servidor TFTP, según el estándar PXE. Si utiliza PXELINUX para arrancar el instalador de ESXi, el archivo binario `pxelinux.0`, `mboot.c32`, el archivo de configuración, el kernel y otros archivos se transfieren mediante TFTP.

Nota VMware compila el complemento `mboot.c32` para que funcione con la versión 3.86 de SYSLINUX y prueba el arranque PXE solo con esa versión. Otras versiones podrían ser incompatibles. *El paquete de divulgación de código abierto para VMware vSphere Hypervisor* incluye correcciones de errores para la versión 3.86 de SYSLINUX.

iPXE

iPXE es un software de código abierto que proporciona una implementación de HTTP. Puede utilizar el software para realizar un arranque inicial. Para obtener más información, consulte https://ipxe.org/.

VMware incluye una compilación de iPXE como parte de Auto Deploy. El árbol de origen de esta compilación está disponible en *el paquete de divulgación de código abierto para VMware vCenter Server*.

UEFI PXE y UEFI HTTP

La mayoría del firmware UEFI es compatible de forma nativa con PXE, lo que permite arrancar desde un servidor TFTP. El firmware puede cargar directamente el cargador de arranque de ESXi para los sistemas UEFI, `mboot.efi`. No es necesario ningún software adicional (p. ej., PXELINUX).

Algunos firmware UEFI son compatibles con el arranque HTTP UEFI nativo. La función se introdujo en la versión 2.5 de la especificación UEFI. El firmware puede cargar el cargador de arranque de ESXi desde un servidor HTTP, sin software adicional, como iPXE.

Nota Los productos Apple Macintosh no son compatibles con el arranque PXE. En cambio, son compatibles con el arranque de red mediante un protocolo específico para Apple.

Métodos alternativos para el arranque de red

También existen métodos alternativos para el arranque de red de software y hosts distintos, por ejemplo:

- Configuración del servidor DHCP para que proporcione diferentes nombres de archivo del cargador de arranque inicial a distintos hosts según la dirección MAC u otros criterios. Consulte la documentación del servidor DCHP.
- Métodos que utilizan iPXE como cargador de arranque inicial con un archivo de configuración de iPXE que selecciona el siguiente cargador de arranque según la dirección MAC u otros criterios.

Archivos de configuración PXELINUX

Se necesita un archivo de configuración PXELINUX para iniciar el instalador de ESXi en un sistema BIOS heredado. El archivo de configuración define el menú que se muestra en el host ESXi de destino a medida que se inicia.

En esta sección, se brinda información general sobre los archivos de configuración PXELINUX.

Para conocer detalles de la sintaxis, visite el sitio web de SYSLINUX en http://www.syslinux.org/.

Archivos requeridos

En el archivo de configuración de PXE, debe incluir rutas de acceso a los siguientes archivos:

- `mboot.c32` es el cargador de arranque.
- `boot.cfg` es el archivo de configuración del cargador de arranque.

Consulte Acerca del archivo boot.cfg .

Nombre del archivo de configuración de PXE

Para el nombre del archivo de configuración de PXE, seleccione una de las siguientes opciones:

- `01-`*`dirección_MAC_del_host_ESXi_de_destino`*. Por ejemplo, `01-23-45-67-89-0a-bc`
- La dirección IP del host ESXi de destino en anotación hexadecimal.
- `default`

El archivo de arranque inicial, `pxelinux.0`, intenta cargar un archivo de configuración de PXE en el siguiente orden:

1 Intenta con la dirección MAC del host ESXi de destino, con su código de tipo ARP, que es 01 para Ethernet, como prefijo.

2 Si ese intento genera un error, intenta con la anotación hexadecimal de la dirección IP del sistema ESXi de destino.

3 Por último, intenta cargar un archivo con el nombre `default`.

Ubicación del archivo de configuración de PXE

Guarde el archivo en `/tftpboot/pxelinux.cfg/` en el servidor TFTP.

Por ejemplo, es posible guardar el archivo en el servidor TFTP en `/tftpboot/pxelinux.cfg/01-00-21-5a-ce-40-f6`. La dirección MAC del adaptador de red del host ESXi de destino es 00-21-5a-ce-40-f6.

Arrancar el instalador de ESXi mediante PXE y TFTP

Es posible utilizar un servidor TFTP para arrancar con PXE el instalador de ESXi. El proceso varía levemente si se utiliza UEFI o el arranque desde un BIOS heredado.

- En los equipos con BIOS heredado, el procedimiento admite el arranque de varias versiones del instalador de ESXi con el mismo cargador de arranque inicial `pxelinux.0` para todos los equipos de destino, pero con archivos de configuración PXELINUX potencialmente diferentes según la dirección MAC de los equipos de destino.
- En los equipos con UEFI, el procedimiento admite el arranque de varias versiones diferentes del instalador de ESXi con el mismo cargador de arranque inicial `mboot.efi` para todos los equipos de destino, pero con archivos `boot.cfg` potencialmente diferentes según la dirección MAC de los equipos de destino.

Requisitos previos

Puesto que la mayoría de los entornos contienen tanto hosts ESXi compatibles con el arranque UEFI como hosts compatibles solo con el BIOS heredado, en este tema se analizan los requisitos previos y los pasos para ambos tipos de hosts.

Compruebe que el entorno cumpla con los siguientes requisitos previos.

- Imagen ISO del instalador de ESXi descargada del sitio web de VMware.
- Host de destino con una configuración de hardware que sea compatible con la versión de ESXi. Consulte la *Guía de compatibilidad de VMware*.
- Un adaptador de red compatible con PXE en el host ESXi de destino.
- Servidor DHCP que puede configurar para el arranque PXE. Consulte Configuraciones de DHCP de muestra.
- Servidor TFTP.

- Directivas de seguridad de red para permitir el tráfico TFTP (Puerto UDP 69).
- Para BIOS heredado, solo se pueden usar redes IPv4. Para el arranque PXE con UEFI, se pueden usar redes IPv4 o IPv6.
- (Opcional) Un script de instalación (archivo de inicio).
- En la mayoría de los casos debe usar una VLAN nativa. Si desea especificar el identificador de la VLAN que se va a utilizar con el arranque PXE, compruebe que su NIC admita la especificación de identificador de la VLAN.

Para los sistemas BIOS heredados, obtenga la versión 3.86 del paquete SYSLINUX. Para obtener más información, consulte Información sobre el arranque de red.

Procedimiento

1 Si el host ESXi ejecuta únicamente el firmware de BIOS heredado, obtenga y configure PXELINUX.

   a Obtenga la versión 3.86 de SYSLINUX, descomprima el paquete y copie el archivo `pxelinux.0` en el directorio de nivel superior `/tftpboot` de su servidor TFTP.

   b Cree un archivo de configuración PXELINUX con el siguiente modelo de código.

   `ESXi-8.x.x-XXXXXX` es el nombre del subdirectorio TFTP donde se encuentran los archivos del instalador de ESXi.

```
DEFAULT install
NOHALT 1
LABEL install
  KERNEL ESXi-8.x.x-XXXXXX/mboot.c32
  APPEND -c ESXi-8.x.x-XXXXXX/boot.cfg
  IPAPPEND 2
```

   c Guarde el archivo PXELINUX en el directorio `/tftpboot/pxelinux.cfg` de su servidor TFTP con un nombre de archivo que determine si todos los hosts arrancarán este instalador de forma predeterminada:

Opción	Descripción
Mismo instalador	Use el nombre `default` para el archivo si desea que todos los hosts arranquen este instalador de ESXi de forma predeterminada.
Diferentes instaladores	Use la dirección MAC del equipo host de destino (01-*dirección_MAC_del_host_ESXi_de_destino*) como nombre para el archivo si desea que solo un host específico arranque con este archivo (por ejemplo, `01-23-45-67-89-0a-bc`).

2 Si el host ESXi ejecuta firmware UEFI, copie los archivos `efi/boot/bootx64.efi` y `efi/boot/crypto64.efi` desde la imagen ISO del instalador de ESXi a la carpeta `/tftpboot` en el servidor TFTP.

3 Cambie el nombre del archivo `efi/boot/bootx64.efi` a `mboot.efi`.

Nota Generalmente, las versiones más recientes de `mboot.efi` pueden arrancar versiones anteriores de ESXi, pero es posible que las versiones anteriores de `mboot.efi` no puedan arrancar versiones más recientes de ESXi. Si desea configurar diversos hosts de manera que arranquen diferentes versiones del instalador de ESXi, utilice el archivo `mboot.efi` de la versión más reciente.

---

4 Configure el servidor DHCP.

5 Cree un subdirectorio en el directorio de nivel superior del servidor TFTP `/tftpboot` con el nombre de la versión de ESXi que almacenará, por ejemplo, `/tftpboot/ESXi-8.x.x-xxxxx`.

6 Copie el contenido de la imagen del instalador de ESXi en el directorio que acaba de crear.

7 Modifique el archivo `boot.cfg`.

  a Agregue la siguiente línea:

```
prefix=ESXi-8.x.x-xxxxxx
```

  Aquí, `ESXi-8.x.x-xxxxxx` es el nombre de la ruta de acceso de los archivos del instalador en el directorio raíz del servidor TFTP.

  b Si los nombres de archivo en las líneas `kernel=` y `modules=` comienzan con un carácter de barra diagonal (/), elimine ese carácter.

  c Si la línea de `kernelopt=` contiene la cadena `cdromBoot`, quite únicamente la cadena.

8 (opcional) En el caso de una instalación generada por script, en el archivo `boot.cfg`, agregue la opción `kernelopt` en la línea siguiente al comando del kernel, para especificar la ubicación del script de instalación.

Utilice el siguiente código como modelo, donde `XXX.XXX.XXX.XXX` es la dirección IP del servidor en el que reside el script de instalación y `esxi_ksFiles` es el directorio que contiene el archivo `ks.cfg`.

```
kernelopt=ks=http://XXX.XXX.XXX.XXX/esxi_ksFiles/ks.cfg
```

9 Si el host ESXi ejecuta el firmware UEFI, especifique si desea que todos los hosts UEFI arranquen el mismo instalador.

Opción	Descripción
Mismo instalador	Copie el archivo `boot.cfg` en `/tftpboot/boot.cfg` o vincúlelo a esta ruta.
Diferentes instaladores	a Cree un subdirectorio de `/tftpboot` con la dirección MAC del equipo host de destino (01-*dirección_MAC_del_host_ESXi_de_destino*) como nombre (por ejemplo, `01-23-45-67-89-0a-bc`). b Coloque una copia (o un vínculo) del archivo `boot.cfg` del host en ese directorio (por ejemplo, `/tftpboot/01-23-45-67-89-0a-bc/boot.cfg`).

Arrancar el instalador de ESXi mediante iPXE y HTTP

Puede usar iPXE para arrancar el instalador de ESXi desde un servidor HTTP.

- En los equipos con BIOS heredado, el procedimiento admite el arranque de varias versiones del instalador de ESXi con el mismo cargador de arranque inicial `pxelinux.0` para todos los equipos de destino, pero con archivos de configuración PXELINUX potencialmente diferentes según la dirección MAC de los equipos de destino.
- En los equipos con UEFI, el procedimiento admite el arranque de varias versiones diferentes del instalador de ESXi con el mismo cargador de arranque inicial `mboot.efi` para todos los equipos de destino, pero con archivos `boot.cfg` potencialmente diferentes según la dirección MAC de los equipos de destino.

Requisitos previos

Los requisitos previos y los pasos dependen solo de la compatibilidad con el arranque UEFI o el BIOS heredado. iPXE se puede utilizar para arrancar el instalador de ESXi desde un servidor HTTP. El siguiente tema analiza los requisitos previos y los pasos para hosts ESXi que admiten el arranque UEFI y los hosts que solo admiten la BIOS heredada.

Compruebe que el entorno tenga los siguientes componentes:

- Imagen ISO del instalador de ESXi descargada del sitio web de VMware.
- Host de destino con una configuración de hardware que sea compatible con la versión de ESXi. Consulte la *Guía de compatibilidad de VMware*.
- Un adaptador de red compatible con PXE en el host ESXi de destino.
- Servidor DHCP que puede configurar para el arranque PXE. Consulte Configuraciones de DHCP de muestra.
- Servidor TFTP.
- Directivas de seguridad de red para permitir el tráfico TFTP (Puerto UDP 69).
- Para BIOS heredado, solo se pueden usar redes IPv4. Para el arranque PXE con UEFI, se pueden usar redes IPv4 o IPv6.
- (Opcional) Un script de instalación (archivo de inicio).
- En la mayoría de los casos debe usar una VLAN nativa. Si desea especificar el identificador de la VLAN que se va a utilizar con el arranque PXE, compruebe que su NIC admita la especificación de identificador de la VLAN.

Asegúrese de que el entorno también cumpla los siguientes requisitos previos para el arranque PXE mediante un servidor HTTP:

- Compruebe que los hosts ESXi de destino puedan acceder al servidor HTTP.
- Si el host ESXi ejecuta únicamente el firmware de BIOS heredado, obtenga la versión 3.86 del paquete SYSLINUX. Para obtener más información, consulte Información sobre el arranque de red.

Procedimiento

1 Obtenga y configure iPXE.

   a Obtenga el código fuente de iPXE.

   b En la página de descarga de iPXE, siga las instrucciones de compilación, pero ejecute uno de los siguientes comandos.

      - En el caso de los hosts ESXi que solo ejecutan el firmware de BIOS heredado, ejecute `make bin/undionly.kpxe`.
      - Para los hosts ESXi que ejecuten el firmware UEFI, ejecute `make bin-x86_64-efi/snponly.efi`.

   c Copie el archivo `undionly.kpxe` o `snponly.efi` al directorio `/tftpboot` del servidor TFTP.

2 Si el host ESXi ejecuta únicamente el firmware de BIOS heredado, obtenga y configure PXELINUX.

   a Obtenga la versión 3.86 de SYSLINUX, descomprima el paquete y copie el archivo `pxelinux.0` en el directorio `/tftpboot` de su servidor TFTP.

   b Cree un archivo de configuración PXELINUX con el siguiente modelo de código.

   `ESXi-8.x.x-XXXXXX` es el nombre del subdirectorio TFTP donde se encuentran los archivos del instalador de ESXi.

```
DEFAULT install
NOHALT 1
LABEL install
  KERNEL ESXi-8.x.x-XXXXXX/mboot.c32
  APPEND -c ESXi-8.x.x-XXXXXX/boot.cfg
  IPAPPEND 2
```

   c Guarde el archivo PXELINUX en el directorio `/tftpboot/pxelinux.cfg` del servidor TFTP.

   El nombre de archivo determina si todos los hosts arrancarán este instalador de forma predeterminada.

Opción	Descripción
Mismo instalador	Use el nombre `default` para el archivo si desea que todos los hosts arranquen este instalador de ESXi de forma predeterminada.
Diferentes instaladores	Asigne un nombre al archivo con la dirección MAC del equipo host de destino (01-*dirección_mac_de_host_ESXi_destino*), si solo un host específico debe arrancar este archivo. Por ejemplo, `01-23-45-67-89-0a-bc`.

3 Si el host ESXi ejecuta el firmware UEFI, copie el archivo `efi/boot/bootx64.efi` desde la imagen ISO del instalador de ESXi en la carpeta `/tftpboot` del servidor TFTP y cambie el nombre del archivo a `mboot.efi`.

Nota Generalmente, las versiones más recientes de `mboot.efi` pueden arrancar versiones anteriores de ESXi, pero es posible que las versiones anteriores de `mboot.efi` no puedan arrancar versiones más recientes de ESXi. Si desea configurar diversos hosts de manera que arranquen diferentes versiones del instalador de ESXi, utilice el archivo `mboot.efi` de la versión más reciente.

---

4 Configure el servidor DHCP.

5 Cree un directorio en el servidor HTTP que tenga el mismo nombre que la versión de ESXi que contendrá. Por ejemplo, `/var/www/html/ESXi-8.x.x-XXXXXX`.

6 Copie el contenido de la imagen del instalador de ESXi en el directorio que acaba de crear.

7 Modifique el archivo `boot.cfg`.

a Agregue la siguiente línea:

```
prefix=http://XXX.XXX.XXX.XXX/ESXi-8.x.x-XXXXXX
```

En la línea superior, `http://XXX.XXX.XXX.XXX/ESXi-8.x.x-XXXXXX` es la ubicación de los archivos del instalador en el servidor HTTP.

b Si los nombres de archivo en las líneas `kernel=` y `modules=` comienzan con un carácter de barra diagonal (/), elimine ese carácter.

c Si la línea de `kernelopt=` contiene la cadena `cdromBoot`, quite únicamente la cadena.

8 (opcional) En el caso de una instalación generada por script, en el archivo `boot.cfg`, agregue la opción `kernelopt` en la línea siguiente al comando del kernel, para especificar la ubicación del script de instalación.

Utilice el siguiente código como modelo, donde `XXX.XXX.XXX.XXX` es la dirección IP del servidor en el que reside el script de instalación y `esxi_ksFiles` es el directorio que contiene el archivo `ks.cfg`.

```
kernelopt=ks=http://XXX.XXX.XXX.XXX/esxi_ksFiles/ks.cfg
```

9 Si el host ESXi ejecuta el firmware UEFI, especifique si desea que todos los hosts UEFI arranquen el mismo instalador.

Opción	Descripción
Mismo instalador	Copie el archivo `boot.cfg` en `/tftpboot/boot.cfg` o vincúlelo a esta ruta.
Diferentes instaladores	a Cree un subdirectorio de `/tftpboot` con la dirección MAC del equipo host de destino (01-*dirección_MAC_del_host_ESXi_de_destino*) como nombre (por ejemplo, `01-23-45-67-89-0a-bc`). b Coloque una copia (o un vínculo) del archivo `boot.cfg` del host en ese directorio (por ejemplo, `/tftpboot/01-23-45-67-89-0a-bc/boot.cfg`).

Arrancar el instalador de ESXi mediante HTTP de UEFI nativo

El instalador de ESXi se puede arrancar directamente desde un servidor HTTP, sin necesidad de disponer de software adicional para admitir el proceso.

HTTP de UEFI permite arrancar varias versiones del instalador de ESXi. Se utiliza el mismo cargador de arranque inicial `mboot.efi` para todos los equipos de destino, pero potencialmente diferentes archivos `boot.cfg` en función de la dirección MAC del equipo de destino.

Nota No mezcle las redes IPv4 o IPv6 durante el proceso de arranque. Utilice solo una de ellas.

Requisitos previos

Compruebe que el entorno tenga los siguientes componentes:

- Un host ESXi con firmware UEFI que admita la función de arranque HTTP.
- Imagen ISO del instalador de ESXi descargada del sitio web de VMware.
- Host de destino con una configuración de hardware que sea compatible con la versión de ESXi. Consulte la *Guía de compatibilidad de VMware*.
- Un adaptador de red compatible con redes UEFI en el host ESXi de destino.
- Un servidor DHCP que podrá configurar para el arranque HTTP de UEFI. Consulte Configuraciones de DHCP de muestra.
- (Opcional) Un script de instalación (archivo de inicio).
- En la mayoría de los casos debe usar una VLAN nativa. Si desea especificar el identificador de la VLAN que se va a utilizar con el arranque PXE, compruebe que su NIC admita la especificación de identificador de la VLAN.

Procedimiento

1 Copie el archivo `efi/boot/bootx64.efi` desde la imagen ISO del instalador de ESXi en un directorio del servidor HTTP y cambie el nombre del archivo a `mboot.efi`. Por ejemplo, `http://www.example.com/esxi/mboot.efi`.

Nota Generalmente, las versiones más recientes de `mboot.efi` pueden arrancar versiones anteriores de ESXi, pero es posible que las versiones anteriores de `mboot.efi` no puedan arrancar versiones más recientes de ESXi. Si desea configurar diversos hosts de manera que arranquen diferentes versiones del instalador de ESXi, utilice el archivo `mboot.efi` de la versión más reciente.

2 Configure el servidor DHCP.

3 Cree un directorio en el servidor HTTP que tenga el mismo nombre que la versión de ESXi que contendrá. Por ejemplo, `http://www.example.com/esxi/ESXi-8.x.x-XXXXXX`.

4 Copie el contenido de la imagen del instalador de ESXi en el directorio que acaba de crear.

5 Modifique el archivo `boot.cfg`.

a Agregue la siguiente línea con la dirección URL del directorio que acaba de crear.

```
prefix=http://www.example.com/esxi/ESXi-8.x.x-XXXXXX
```

b Si los nombres de archivo en las líneas `kernel=` y `modules=` comienzan con un carácter de barra diagonal (/), elimine ese carácter.

c Si la línea de `kernelopt=` contiene la cadena `cdromBoot`, quite únicamente la cadena.

6 (opcional) En el caso de una instalación generada por script, en el archivo `boot.cfg`, agregue la opción `kernelopt` en la línea siguiente al comando del kernel, para especificar la ubicación del script de instalación.

Por ejemplo, `kernelopt=ks=http://www.example.com/esxi_ksFiles/ks.cfg`

7 (opcional) Puede utilizar los parámetros de configuración de la máquina virtual *networkBootProtocol* y *networkBootUri* para especificar desde dónde se puede arrancar una máquina virtual. La opción *networkBootProtocol* especifica el protocolo de arranque, IPv4 o IPv6. Por ejemplo, `networkBootProtocol = httpv4`. La opción *networkBootUri* especifica la URL HTTP del cargador de arranque ESXi (bootx64.efi). Por ejemplo, `networkBootUri = http://xxx.xxx.xx.x/esxi80uc1/efi/boot/bootx64.efi`.

8 Especifique si desea que todos los hosts UEFI arranquen el mismo instalador.

Opción	Descripción
Mismo instalador	Agregue el archivo `boot.cfg` al mismo directorio que `mboot.efi`. Por ejemplo, `http://www.example.com/esxi/boot.cfg`
Diferentes instaladores	a Cree un subdirectorio del directorio que contenga el archivo `mboot.efi`. Asigne un nombre al directorio que sea como la dirección MAC del equipo host de destino (01-*dirección_mac_de_host_ESXi_destino*); por ejemplo, `01-23-45-67-89-0a-bc`. b Agregue el archivo `boot.cfg` personalizado al directorio. Por ejemplo, `http://www.example.com/esxi/01-23-45-67-89-0a-bc/boot.cfg`.

Puede utilizar ambos tipos de instalador. Los hosts ESXi que no tengan un archivo `boot.cfg` personalizado en el servidor HTTP, arranque desde el archivo `boot.cfg` predeterminado.

Configuraciones de DHCP de muestra

El servidor DHCP debe enviar la dirección del servidor TFTP o HTTP, y el nombre de archivo del cargador de arranque inicial al host ESXi.

Cuando la máquina de destino arranca por primera vez, transmite un paquete mediante la red para solicitar información a fin de realizar el arranque por sí misma. El servidor DHCP responde. El servidor DHCP debe ser capaz de determinar si la máquina de destino puede arrancar y, asimismo, de determinar la ubicación del archivo binario del cargador de arranque inicial. Para el arranque PXE, la ubicación es un archivo en un servidor TFTP. Para el arranque UEFI HTTP, la ubicación es una URL.

Precaución No configure un segundo servidor DHCP si la red ya tiene uno. Si varios servidores DHCP responden a las solicitudes de DHCP, las máquinas pueden obtener direcciones IP incorrectas o en conflicto, o no recibir la información de arranque correcta. Consulte a un administrador de red antes de configurar un servidor DHCP. Para obtener asistencia en relación con la configuración de DHCP, póngase en contacto con el proveedor del servidor DHCP.

Hay muchos servidores DHCP que puede utilizar. Los siguientes ejemplos son para un servidor DHCP de ISC. Si usa una versión de DHCP para Microsoft Windows, consulte la documentación del servidor DHCP para determinar cómo transmitir los argumentos `next-server` y `filename` a la máquina de destino.

Ejemplo de arranque mediante PXE y TFTP con IPv4

En este ejemplo se muestra cómo configurar un servidor DHCP de ISC para el arranque PXE de ESXi mediante un servidor TFTP en una dirección IPv4 xxx.xxx.xxx.xxx.

```
#
# ISC DHCP server configuration file snippet.  This is not a complete
# configuration file; see the ISC server documentation for details on
# how to configure the DHCP server.
#
allow booting;
```

```
allow bootp;
option client-system-arch code 93 = unsigned integer 16;
class "pxeclients" {
   match if substring(option vendor-class-identifier, 0, 9) = "PXEClient";
   next-server xxx.xxx.xxx.xxx;
   if option client-system-arch = 00:07 or option client-system-arch = 00:09 {
      filename = "mboot.efi";
   } else {
      filename = "pxelinux.0";
   }
}
```

Cuando una máquina intenta realizar un arranque PXE, el servidor DHCP proporciona una dirección IP y la ubicación del archivo binario `pxelinux.0` o `mboot.efi` en el servidor TFTP.

Ejemplo de arranque mediante PXE y TFTP con IPv6

En este ejemplo se muestra cómo configurar un servidor DHCPv6 de ISC para el arranque PXE de ESXi mediante un servidor TFTP en una dirección IPv6 xxxx:xxxx:xxxx:xxxx::xxxx.

```
#
# ISC DHCPv6 server configuration file snippet.  This is not a complete
# configuration file; see the ISC server documentation for details on
# how to configure the DHCP server.
#
allow booting;
allow bootp;
option dhcp6.bootfile-url code 59 = string;
option dhcp6.bootfile-url "tftp://[xxxx:xxxx:xxxx:xxxx::xxxx]/mboot.efi";
```

Cuando una máquina intenta realizar un arranque PXE, el servidor DHCP proporciona una dirección IP y la ubicación del archivo binario `mboot.efi` en el servidor TFTP.

Ejemplo de arranque mediante iPXE y HTTP con IPv4

En este ejemplo se muestra cómo configurar un servidor DHCP de ISC para arrancar ESXi mediante la carga de iPXE desde un servidor TFTP en una dirección IPv4 `xxx.xxx.xxx.xxx`.

```
#
# ISC DHCP server configuration file snippet.  This is not a complete
# configuration file; see the ISC server documentation for details on
# how to configure the DHCP server.
#
allow booting;
allow bootp;
option client-system-arch code 93 = unsigned integer 16;
class "pxeclients" {
   match if substring(option vendor-class-identifier, 0, 9) = "PXEClient";
   next-server xxx.xxx.xxx.xxx;
   if option client-system-arch = 00:07 or option client-system-arch = 00:09 {
      if exists user-class and option user-class = "iPXE" {
         # Instruct iPXE to load mboot.efi as secondary bootloader
         filename = "mboot.efi";
      } else {
```

```
         # Load the snponly.efi configuration of iPXE as initial bootloader
         filename = "snponly.efi";
      }
   } else {
      if exists user-class and option user-class = "iPXE" {
         # Instruct iPXE to load pxelinux as secondary bootloader
         filename = "pxelinux.0";
      } else {
         # Load the undionly configuration of iPXE as initial bootloader
         filename = "undionly.kpxe";
   }
}
```

Cuando una máquina intenta realizar un arranque PXE, el servidor DHCP proporciona una dirección IP y la ubicación del archivo binario `undionly.kpxe` o `snponly.efi` en el servidor TFTP. En el caso de BIOS heredado, iPXE pide al servidor DHCP el siguiente archivo que se debe cargar y el servidor devuelve el nombre de archivo `pxelinux.0`. En el caso de UEFI, iPXE pide al servidor DHCP el siguiente archivo que se debe cargar y, en esta ocasión, el servidor devuelve el nombre de archivo `mboot.efi`. En ambos casos, iPXE es residente, y el sistema tiene la capacidad HTTP. Como resultado, el sistema puede cargar archivos adicionales desde un servidor HTTP.

Ejemplo de arranque mediante iPXE y HTTP con IPv6

En este ejemplo se muestra cómo configurar un servidor DHCPv6 de ISC para arrancar ESXi mediante la carga de iPXE desde un servidor TFTP en una dirección IPv6 `xxxx:xxxx:xxxx:xxxx::xxxx`.

```
#
# ISC DHCPv6 server configuration file snippet.  This is not a complete
# configuration file; see the ISC server documentation for details on
# how to configure the DHCP server.
#
allow booting;
allow bootp;

option dhcp6.bootfile-url code 59 = string;
if exists user-class and option user-class = "iPXE" {
   # Instruct iPXE to load mboot.efi as secondary bootloader
   option dhcp6.bootfile-url "tftp://[xxxx:xxxx:xxxx:xxxx::xxxx]/mboot.efi";
} else {
   # Load the snponly.efi configuration of iPXE as initial bootloader
   option dhcp6.bootfile-url "tftp://[xxxx:xxxx:xxxx:xxxx::xxxx]/snponly.efi";
}
```

Cuando una máquina intenta realizar un arranque PXE, el servidor DHCP proporciona una dirección IP y la ubicación del archivo binario `snponly.efi` (iPXE) en el servidor TFTP. iPXE pide al servidor DHCP el siguiente archivo que se debe cargar y, en esta ocasión, el servidor devuelve el nombre de archivo `mboot.efi`. iPXE es residente y el sistema tiene la capacidad HTTP. Como resultado, el sistema puede cargar archivos adicionales desde un servidor HTTP.

Ejemplo de arranque mediante UEFI HTTP con IPv4

En este ejemplo se muestra cómo configurar un servidor DHCP de ISC para arrancar ESXi mediante el uso de UEFI HTTP nativo en IPv4 desde el servidor web `www.example.com`.

```
#
# ISC DHCP server configuration file snippet.  This is not a complete
# configuration file; see the ISC server documentation for details on
# how to configure the DHCP server.
#
allow booting;
allow bootp;
option client-system-arch code 93 = unsigned integer 16;
class "httpclients" {
   match if substring(option vendor-class-identifier, 0, 10) = "HTTPClient";
   option vendor-class-identifier "HTTPClient";

   if option client-system-arch = 00:10 {
      # x86_64 UEFI HTTP client
      filename = http://www.example.com/esxi/mboot.efi;
   }
}
```

Ejemplo de arranque mediante UEFI HTTP con IPv6

En este ejemplo se muestra cómo configurar un servidor DHCPv6 de ISC para que arranque ESXi mediante el uso de HTTP UEFI nativo en IPv6 desde el servidor web `www.example.com`.

```
#
# ISC DHCPv6 server configuration file snippet.  This is not a complete
# configuration file; see the ISC server documentation for details on
# how to configure the DHCP server.
#
allow booting;
allow bootp;

option dhcp6.bootfile-url code 59 = string;
option dhcp6.user-class code 15 = { integer 16, string };
option dhcp6.vendor-class code 16 = { integer 32, integer 16, string };

if option dhcp6.client-arch-type = 00:10 {
      # x86_64 HTTP clients
      option dhcp6.vendor-class 0 10 "HTTPClient";
      option dhcp6.bootfile-url "http://www.example.com/esxi/mboot.efi";
}
```

Instalar ESXi con vSphere Auto Deploy

vSphere Auto Deploy permite aprovisionar cientos de hosts físicos con el software ESXi.

Mediante el uso de Auto Deploy, los administradores de sistemas experimentados pueden administrar de forma eficiente implementaciones grandes. Los hosts se arrancan mediante la red desde un servidor Auto Deploy central. De forma opcional, se configuran los hosts con un perfil de host de un host de referencia. El perfil de host se puede configurar para que le solicite al usuario información. Después que concluya el arranque y la configuración, los hosts los administra vCenter Server al igual que otros hosts ESXi.

Auto Deploy también se puede utilizar para almacenamientos en caché sin estado o instalaciones con estado.

Importante Auto Deploy requiere una separación segura entre la red de producción y las redes de administración o implementación, según se describe en Consideraciones de seguridad de vSphere Auto Deploy. No es seguro utilizar Auto Deploy sin esta separación.

Almacenamiento en caché sin estado

De manera predeterminada, Auto Deploy no almacena la configuración o estado de ESXi en el disco host. En su lugar, un perfil de imagen define la imagen con la que se aprovisiona el host. Los otros atributos de host se administran mediante perfiles de host. El host que utiliza Auto Deploy para el almacenamiento en caché sin estado debe conectarse al servidor Auto Deploy y a vCenter Server.

Instalaciones con estado

Puede aprovisionar un host con Auto Deploy y configurar el host para que almacene la imagen en el disco. En los arranques posteriores, el host lo hará desde el disco.

Información sobre vSphere Auto Deploy

vSphere Auto Deploy puede aprovisionar cientos de hosts físicos con el software ESXi.

Se puede especificar la imagen que se implementará y los hosts que se aprovisionarán con esa imagen. Opcionalmente, puede especificar perfiles para aplicar a los hosts, una ubicación de vCenter Server (centro de datos, carpeta o clúster) y asignar un paquete de scripts para cada host.

Introducción a vSphere Auto Deploy

vSphere Auto Deploy utiliza la infraestructura de arranque PXE con perfiles de host, una imagen deseada o una configuración en un nivel de clúster para aprovisionar hosts ESXi.

Información de estado de hosts ESXi

Nota No puede usar Auto Deploy en hosts ESXi configurados con DPU como parte de la función vSphere Distributed Services Engine.

Cuando se inicia un host físico configurado para vSphere Auto Deploy, vSphere Auto Deploy usa la infraestructura de arranque PXE junto con perfiles de host de vSphere, una imagen deseada o una configuración a nivel de clúster para aprovisionar y personalizar ese host. No se almacena ningún estado en el propio host. En su lugar, el servidor vSphere Auto Deploy administra la

información de estado de cada host. vSphere Auto Deploy almacena la información de los hosts ESXi que se van a aprovisionar en distintas ubicaciones. La información sobre la ubicación de los perfiles de imagen, los perfiles de host o los clústeres que administra mediante una sola imagen o mediante una configuración a nivel de clúster se especifica inicialmente en las reglas que asignan máquinas a perfiles de imagen y perfiles de host.

Tabla 4-16. vSphere Auto Deploy almacena información de implementación

Tipo de información	Descripción	Origen de información
Estado de imagen	El software ejecutable que se va a ejecutar en un host ESXi.	Perfil de imagen creado con vSphere ESXi Image Builder o una imagen de vSphere Lifecycle Manager.
Estado de configuración	Los parámetros que se pueden configurar, los cuales determinan el modo en que se configura el host; por ejemplo, conmutadores virtuales y su configuración, configuración de controladores y parámetros de arranque, etc.	Perfil de host creado mediante la interfaz de usuario del perfil de host o una configuración que se crea al configurar un clúster que administra todas las opciones del host ESXi a nivel de clúster en la interfaz de usuario de Inventory.
Estado dinámico	El estado de tiempo de ejecución que genera el software en ejecución; por ejemplo, claves privadas generadas o bases de datos de tiempo de ejecución.	Memoria de host, que se pierde durante el reinicio.
Estado de máquina virtual	Las máquinas virtuales almacenadas en un host y la información de inicio automático de máquinas virtuales (solo arranques posteriores).	La información de máquinas virtuales que envía vCenter Server a vSphere Auto Deploy debe estar disponible para suministrar información de máquinas virtuales a vSphere Auto Deploy.
Intervención del usuario	El estado basado en la intervención del usuario (por ejemplo, una dirección IP que el usuario proporciona cuando se inicia el sistema) no se puede incluir automáticamente en el perfil de host.	Información de personalización del host, almacenada por vCenter Server durante el primer arranque. Puede crear un perfil de host que requiera la intervención del usuario para determinados valores. Cuando vSphere Auto Deploy aplica un perfil de host para el que se requiere información que proporcionó el usuario, el host se coloca en modo de mantenimiento. Utilice la interfaz de usuario del perfil de host para comprobar el cumplimiento del perfil de host y responda al aviso para personalizar el host.

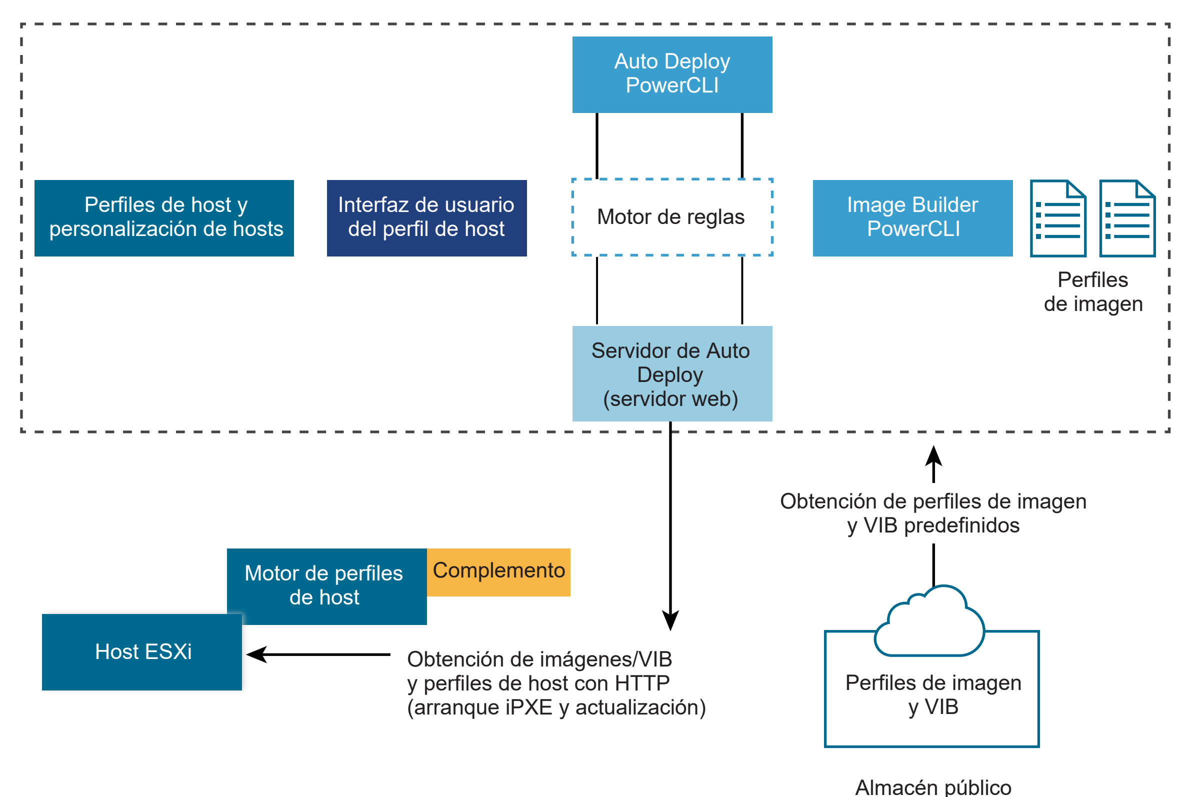
Arquitectura de vSphere Auto Deploy

La infraestructura de vSphere Auto Deploy consta de varios componentes.

Para obtener más información, vea el vídeo "Arquitectura de Auto Deploy":

 (Arquitectura de Auto Deploy)

Figura 4-6. Arquitectura de vSphere Auto Deploy



Servidor vSphere Auto Deploy

Sirve imágenes y perfiles de host a hosts ESXi.

Motor de reglas de vSphere Auto Deploy

Envía información al servidor vSphere Auto Deploy sobre qué perfil de imagen y qué perfil de host asignar a qué host. Los administradores utilizan vSphere Auto Deploy para definir las reglas que asignan perfiles de imagen y perfiles de host a los hosts. Para obtener más información sobre las reglas y los conjuntos de reglas de vSphere Auto Deploy, consulte Reglas y conjuntos de reglas.

Además de los perfiles de imagen heredados que se crean mediante los perfiles de host y VMware Image Builder, también se pueden crear reglas de vSphere Auto Deploy para implementar ESXi mediante una sola imagen de vSphere Lifecycle Manager o una configuración a nivel de clúster.

Perfiles de imagen

Defina el conjunto de VIB para arrancar hosts ESXi.

- VMware y los partners de VMware ponen perfiles de imagen y VIB a disposición en almacenes públicos. Utilice vSphere ESXi Image Builder para examinar el almacén y use el motor de reglas de vSphere Auto Deploy para especificar qué perfil de imagen se debe asignar a qué host.

- Se utilizan imágenes de vSphere Lifecycle Manager para aplicar actualizaciones de software y firmware a los hosts ESXi en un clúster. El uso de una sola imagen para administrar todos los hosts de un clúster garantiza la homogeneidad de la imagen del host en todo el clúster.
- Con ESXi 8.0, puede configurar un clúster que administre toda la configuración del host ESXi a nivel del clúster.
- Los clientes de VMware pueden crear un perfil de imagen personalizado basado en los perfiles de imagen y VIB públicos del almacén y aplicar ese perfil de imagen al host. Consulte Personalizar instalaciones con vSphere ESXi Image Builder.

Perfiles de host

Defina la configuración específica de equipo, como parámetros de red o almacenamiento. Utilice la interfaz de usuario del perfil de host para crear perfiles de host. Puede crear un perfil de host para un host de referencia y aplicar dicho perfil a otros hosts del entorno para obtener una configuración coherente. Para obtener más información, consulte la documentación *Perfiles de host de vSphere* o la sección Configurar un host de referencia de vSphere Auto Deploy.

Personalizar hosts

Almacena información que el usuario proporciona cuando se aplican perfiles de host al host. La personalización de host podría contener direcciones IP u otra información que el usuario suministró para ese host. Para obtener más información sobre la personalización de host, consulte la documentación *Perfiles de host de vSphere*.

En las versiones anteriores de vSphere Auto Deploy, la personalización de host se denominaba archivo de respuesta.

Certificados de Auto Deploy

De manera predeterminada, el servidor Auto Deploy aprovisiona cada host con certificados firmados por VMware Certificate Authority (VMware CA). Para obtener más información, consulte Administrar certificados para hosts ESXi.

Como alternativa, si la directiva corporativa requiere que utilice certificados personalizados, puede configurar el servidor Auto Deploy para aprovisionar a todos los hosts con certificados personalizados que no estén firmados por VMware CA. El servidor Auto Deploy se transforma en una entidad de certificación subordinada a la entidad de certificación externa. En el modo de entidad de certificación personalizada, es responsable de administrar los certificados. No puede actualizar ni renovar certificados desde vSphere Client. En este modo, tampoco puede seleccionar solo un conjunto de hosts para aprovisionarlo con certificados personalizados, y puede firmar manualmente certificados personalizados solo para hosts con estado. Para obtener más información, consulte Usar certificados personalizados con Auto Deploy.

Con ESXi 8.0, Auto Deploy proporciona una tercera opción que le permite generar un certificado aparte de vSphere y pasar a ser independiente de la administración de certificados en vCenter Server. Por ejemplo, puede generar un certificado personalizado mediante un script personalizado o mediante un proveedor de servicios de registro de nombres de dominio, como Verisign. Puede utilizar certificados personalizados solo para un conjunto de hosts ESXi. También puede proporcionar certificados personalizados para hosts sin estado. Los hosts ESXi se identifican mediante la dirección MAC de la NIC que se utiliza para el arranque de red o el UUID del BIOS del host ESXi. VMware Endpoint Certificate Store (VECS) se actualiza con el certificado personalizado mediante PowerCLI. Para obtener más información sobre los nuevos cmdlets de PowerCLI, consulte Descripción general de cmdlets de vSphere Auto Deploy PowerCLI. VMware CA debe confiar en los certificados de ESXi personalizados, por lo que debe agregar el certificado público de CA para los certificados personalizados al almacén de TRUSTED_ROOTS en VECS. Auto Deploy también almacena los certificados personalizados y, cuando reconoce un host de arranque con la dirección MAC correspondiente de la NIC que se ha utilizado para el arranque de red o el UUID del BIOS del host ESXi, proporciona automáticamente el certificado personalizado. No es necesario que detenga o reinicie Auto Deploy ni vCenter Server cuando agregue un certificado personalizado a VECS; solo hay que reiniciar el host para el que cargue un certificado personalizado. Para obtener más información, consulte Usar certificados personalizados con Auto Deploy.

Reglas y conjuntos de reglas

El comportamiento del servidor vSphere Auto Deploy se especifica con un conjunto de reglas. El motor de reglas de vSphere Auto Deploy comprueba el conjunto de reglas para patrones de host coincidentes a fin de decidir con qué elementos (perfil de imagen, perfil de host, ubicación de vCenter Server u objeto de script) se debe aprovisionar cada host.

El motor de reglas asigna parámetros de software y configuración a los hosts según los atributos del host. Por ejemplo, puede implementar perfiles de imagen o perfiles de host a dos clústeres de hosts escribiendo dos reglas, cada una de las cuales debe coincidir con la dirección de red de un clúster.

Para hosts que aún no se han agregado a un sistema vCenter Server, el servidor vSphere Auto Deploy comprueba con el motor de reglas antes de entregar información de perfiles de imagen, perfiles de host y ubicación de inventario a los hosts. Para hosts administrados por un sistema vCenter Server, se usa el perfil de imagen, perfil de host y ubicación de inventario que vCenter Server tiene almacenados en el objeto de host. Si modifica las reglas, puede usar los cmdlets de vSphere Client o vSphere Auto Deploy en una sesión de PowerCLI para probar y reparar el cumplimiento de reglas. Cuando se repara el cumplimiento de reglas para un host, se actualizan las asignaciones de perfil de imagen y perfil de host de ese host.

El motor de reglas incluye reglas y conjuntos de reglas.

Reglas

Las reglas pueden asignar perfiles de imagen y de host a un conjunto de hosts, o bien especificar la ubicación (carpeta o clúster) de un host en el sistema vCenter Server de destino. Una regla puede identificar hosts de destino mediante la dirección MAC de arranque,

la información del SMBIOS, la UUID del BIOS, el proveedor, el modelo o la dirección IP de DHCP fija. En la mayoría de los casos, se aplican reglas a varios hosts. Las reglas se crean mediante los cmdlets de vSphere Client o vSphere Auto Deploy en una sesión de PowerCLI. Después de crear una regla, se la debe agregar a un conjunto de reglas. Solo se admiten dos conjuntos de reglas: el conjunto de reglas activas y el conjunto de reglas de trabajo. Una regla puede pertenecer a ambos conjuntos, al predeterminado o solo al conjunto de reglas de trabajo. Una vez que la regla se agrega a un conjunto de reglas, ya no se puede cambiar. En su lugar, copie la regla y reemplace los elementos o los patrones en la copia. Si administra vSphere Auto Deploy con vSphere Client, puede editar una regla si se encuentra en estado inactivo.

Puede especificar los siguientes parámetros en una regla.

<table>
<tr><th>Parámetro</th><th>Descripción</th></tr>
<tr><td>Nombre</td><td>Nombre de la regla, especificado mediante el parámetro <code>-Name</code>.</td></tr>
<tr><td>Elemento</td><td>Un elemento o más, especificados mediante el parámetro <code>-Item</code>. Un elemento puede ser un perfil de imagen, un perfil de host, una ubicación en el inventario de vCenter Server (centro de datos, carpeta o clúster) para el host de destino o un script personalizado. Puede especificar varios elementos, separados por comas.</td></tr>
<tr><td>Patrón</td><td>El patrón especifica el host o el grupo de hosts a los que se aplica la regla.

vendor
Nombre del proveedor de la máquina.

model
Nombre del modelo de la máquina.

serie
Número de serie de la máquina.

hostname
Nombre de host de la máquina.

domain
Nombre del dominio.

ipv4
Dirección IPv4 de la máquina.

ipv6
Dirección IPv6 de la máquina.
El arranque PXE con firmware de BIOS solo se puede realizar mediante IPv4; el arranque PXE con firmware de UEFI se puede realizar mediante IPv4 o IPv6.

mac
Dirección MAC de NIC de arranque.

asset
Etiqueta de recurso de la máquina.

oemstring
Cadenas específicas del fabricante del equipo original (OEM) en el SMBIOS.

Puede especificar el parámetro <code>-AllHosts</code> para aplicar el elemento o los elementos a todos los hosts.</td></tr>
</table>

Conjunto de reglas activas

Cuando un host iniciado recientemente contacta al servidor vSphere Auto Deploy con una solicitud de perfil de imagen, el servidor vSphere Auto Deploy si hay reglas coincidentes en el conjunto de reglas activas. El perfil de imagen, el perfil de host, la ubicación de inventario de vCenter Server y el objeto de script que se asignan mediante reglas coincidentes se utilizan posteriormente para arrancar el host. Si las reglas asignan más de un elemento del

mismo tipo, el servidor vSphere Auto Deploy utilizará el elemento que aparezca primero en el conjunto de reglas.

Conjunto de reglas de trabajo

El conjunto de reglas de trabajo permite probar cambios en las reglas antes de que se activen dichos cambios. Por ejemplo, puede usar cmdlets de vSphere Auto Deploy para probar el cumplimiento del conjunto de reglas de trabajo. La prueba verifica que los hosts administrados por un sistema vCenter Server sigan las reglas en el conjunto de reglas de trabajo. De manera predeterminada, los cmdlets agregan la regla al conjunto de reglas de trabajo y activan las reglas. Utilice el parámetro `NoActivate` para agregar una regla solamente al conjunto de reglas de trabajo.

Con las reglas y los conjuntos de reglas se usa el siguiente flujo de trabajo.

1 Haga cambios en el conjunto de reglas de trabajo.

2 Pruebe las reglas del conjunto de reglas de trabajo para un host a fin de garantizar que todo funcione correctamente.

3 Refine y vuelva a probar las reglas en el conjunto de reglas de trabajo.

4 Active las reglas en el conjunto de reglas de trabajo.

   Si agrega una regla en una sesión de PowerCLI y no especifica el parámetro `NoActivate`, se activan todas las reglas que se encuentran actualmente en el conjunto de reglas de trabajo. No puede activar reglas individuales.

Consulte la ayuda de la línea de comandos PowerCLI y Administrar vSphere Auto Deploy con cmdlets de PowerCLI para obtener más información sobre el uso de vSphere Auto Deploy con cmdlets de PowerCLI. Consulte Administrar vSphere Auto Deploy con vSphere Client para obtener más información sobre el uso de vSphere Auto Deploy con vSphere Client.

Instalar y configurar vSphere Auto Deploy

Antes de comenzar a usar vSphere Auto Deploy, debe preparar el entorno en varios pasos.

Comience con la configuración de los servidores y la preparación del hardware. Debe configurar el tipo de inicio para el servicio de vSphere Auto Deploy en el sistema vCenter Server que planea utilizar para administrar los hosts que aprovisione, y debe instalar PowerCLI.

Qué leer a continuación

- Lista de comprobación previa a la instalación de vSphere Auto Deploy

  Para poder iniciar las tareas en este escenario de vSphere Auto Deploy, primero debe asegurarse de que el entorno cumpla con los requisitos de hardware y software, y de contar con los permisos necesarios para los componentes que se incluyen en la configuración.

- Preparar el sistema para vSphere Auto Deploy

  Para poder realizar un arranque PXE de un host ESXi con vSphere Auto Deploy, primero es necesario instalar el software de los requisitos previos y configurar los servidores DHCP y TFTP con los que deberá interactuar vSphere Auto Deploy.

- Usar los cmdlets de vSphere Auto Deploy

  Los cmdlets de vSphere Auto Deploy se implementan como cmdlets de Microsoft PowerShell y se incluyen en PowerCLI. Los usuarios de los cmdlets de vSphere Auto Deploy pueden aprovechar todas las funciones de PowerCLI.

- Configurar licencias masivas

  Puede utilizar vSphere Client o ESXi Shell para especificar claves de licencia individuales o configurar licencias masivas mediante los cmdlets de PowerCLI. Las licencias masivas funcionan para todos los hosts ESXi, pero son especialmente útiles para los hosts aprovisionados con vSphere Auto Deploy.

Lista de comprobación previa a la instalación de vSphere Auto Deploy

Para poder iniciar las tareas en este escenario de vSphere Auto Deploy, primero debe asegurarse de que el entorno cumpla con los requisitos de hardware y software, y de contar con los permisos necesarios para los componentes que se incluyen en la configuración.

Tabla 4-17. Lista de verificación previa a la instalación

Software y hardware necesarios	Detalles
vCenter Server	El servidor vSphere Auto Deploy forma parte de vCenter Server. Debe habilitar e iniciar el servicio vSphere Auto Deploy en el sistema vCenter Server. Puede realizar muchas de las tareas de configuración iniciando sesión en vCenter Server. Consulte Preparar el sistema para vSphere Auto Deploy.
Almacenamiento	El almacenamiento para los almacenes de datos NFS, iSCSI o Fibre Channel de ESXi, con servidores y matrices de almacenamiento que se configuran de manera tal que los servidores puedan detectar los LUN. ■ Una lista de las direcciones IP de destino para NFS o iSCSI. ■ Una lista con la información de los volúmenes de destino para NFS o iSCSI.

Tabla 4-17. Lista de verificación previa a la instalación (continuación)

Software y hardware necesarios	Detalles
Información del host (para cuatro hosts ESXi)	Una lista de las direcciones IP de destino para NFS o iSCSI. Una lista con la información de los volúmenes de destino para NFS o iSCSI. ■ La ruta predeterminada, la máscara de red y las direcciones IP de los servidores DNS principales y secundarios. ■ La dirección IP y la máscara de red de la red de administración principal de VMkernel. ■ La dirección IP y la máscara de red de las demás redes de VMkernel, como el almacenamiento, vSphere FT o VMware vMotion. vSphere Auto Deploy no sobrescribe las particiones existentes como opción predeterminada.
PowerCLI	Consulte Instalar PowerCLI.
Almacén de software de ESXi	La ubicación del almacén de software de ESXi en la página de descargas del sitio web de VMware. Se debe usar una URL para apuntar al perfil de imagen que está almacenado en esa ubicación o se debe descargar un archivo .zip que funcione con un almacén local. No descargue la imagen de ESXi.
servidor TFTP	El software del instalador para TFTP, como un servidor TFTP de WinAgents.
Servidor DHCP	El servidor DHCP se incluye en las versiones de vSphere compatibles con Windows Server.
Servidor DNS	Un servidor DNS en funcionamiento. Es necesario agregar entradas tanto en Zona directa (Registro A) como en Zona inversa (Registro PTR) para cada host de destino.

También se necesita información acerca de los privilegios de administrador para los servidores principales del entorno, incluidos el servidor de Active Directory, el servidor DNS, el servidor DHCP, el servidor NTP, etc.

Se debe tener control completo del dominio de difusión de la subred en la que se implementa la configuración. Asegúrese de que no haya otros servidores DHCP, DNS ni TFTP en esta subred.

Preparar el sistema para vSphere Auto Deploy

Para poder realizar un arranque PXE de un host ESXi con vSphere Auto Deploy, primero es necesario instalar el software de los requisitos previos y configurar los servidores DHCP y TFTP con los que deberá interactuar vSphere Auto Deploy.

Si desea administrar vSphere Auto Deploy con cmdlets de PowerCLI, consulte *Configurar vSphere Auto Deploy y aprovisionar hosts con vSphere PowerCLI*.

Requisitos previos

- Compruebe que los hosts que desea aprovisionar con vSphere Auto Deploy cumplan los requisitos de hardware para ESXi. Consulte Requisitos de hardware de ESXi.
- Compruebe que los hosts ESXi tengan conectividad de red con vCenter Server y que se cumplan todos los requisitos de puerto. Consulte *Actualización de vCenter Server*.
- Compruebe que dispone de un servidor TFTP y un servidor DHCP en el entorno para enviar archivos y asignar direcciones de red a los hosts ESXi que aprovisiona Auto Deploy. Consulte Instalar el servidor TFTP y Preparar el servidor DHCP para el aprovisionamiento de vSphere Auto Deploy.
- Compruebe que los hosts ESXi tengan conectividad de red a los servidores DHCP, TFTP y vSphere Auto Deploy.
- Si desea usar redes VLAN en el entorno de vSphere Auto Deploy, debe configurar las redes de extremo a extremo correctamente. Cuando el host realiza un arranque PXE, se debe configurar el controlador de firmware de manera que los marcos se etiqueten con los identificadores de VLAN apropiados. Debe realizar los cambios apropiados en la interfaz UEFI/BIOS de forma manual para establecer esta configuración. De forma similar, debe configurar los grupos de puertos de ESXi correctamente con los identificadores de VLAN adecuados. Póngase en contacto con su administrador de red para obtener más información sobre la manera en la que los identificadores de VLAN se utilizan en el entorno.
- Asegúrese de contar con suficiente espacio de almacenamiento para el repositorio de vSphere Auto Deploy. El servidor vSphere Auto Deploy utiliza el repositorio para almacenar los datos que necesita, incluidos las reglas y los conjuntos de reglas que usted crea, así como los VIB y los perfiles de imagen que se especifican en las reglas.

  Se recomienda asignar 2 GB para que haya suficiente espacio para almacenar cuatro perfiles de imagen y quede espacio adicional. Cada perfil de imagen requiere aproximadamente 400 MB. Determine la cantidad de perfiles de imagen que espera utilizar para definir la cantidad de espacio que debe reservar para el repositorio de vSphere Auto Deploy.
- Otorgue privilegios administrativos al servidor DHCP que administra el segmento de red desde el cual desea realizar el arranque. Puede utilizar un servidor DHCP que ya se encuentre en el entorno, o bien instalarlo. Para la configuración de vSphere Auto Deploy, reemplace el nombre de archivo `gpxelinux.0` con `snponly64.efi.vmw-hardwired` para UEFI o `undionly.kpxe.vmw-hardwired` para BIOS. Para obtener más información sobre las configuraciones de DHCP, consulte Configuraciones de DHCP de muestra.
- Proteja la red como lo haría para cualquier otro método de implementación basado en PXE. vSphere Auto Deploy transfiere datos por SSL para evitar interferencias accidentales e intromisiones. No obstante, la autenticidad del cliente o del servidor vSphere Auto Deploy no se comprueba durante el arranque PXE.
- Si desea administrar vSphere Auto Deploy con cmdlets de PowerCLI, compruebe que Microsoft .NET Framework 4.5 o 4.5.x y Windows PowerShell 3.0 o 4.0 se encuentren instalados en un equipo Windows. Consulte *Guía del usuario de vSphere PowerCLI*.

- Configure un servidor remoto de Syslog. Consulte la documentación de *Administrar vCenter Server y hosts* para obtener información sobre la configuración del servidor de Syslog. Configure el primer host que arranque para que use el servidor remoto de Syslog y aplique el perfil de host de dicho host a todos los demás hosts de destino. De forma opcional, instale y utilice VMware vCenter Log Insight, que proporciona agregación y análisis de registros para productos VMware y productos que no son VMware, virtuales y físicos, con búsqueda y análisis de eventos de registro casi en tiempo real.
- Instale ESXi Dump Collector, configure el primer host de manera que todos los volcados de memoria del núcleo se direccionen a ESXi Dump Collector y aplique el perfil de host de ese host a todos los otros hosts. Consulte Configurar ESXi Dump Collector con ESXCLI .
- Si los hosts que planea aprovisionar con vSphere Auto Deploy presentan un BIOS heredado, compruebe que el servidor vSphere Auto Deploy tenga una dirección IPv4. El arranque PXE con firmware de BIOS heredado solo se puede realizar mediante IPv4. El arranque PXE con firmware UEFI se puede realizar mediante IPv4 o IPv6.

Procedimiento

1 Desplácese hasta **Inicio > Auto Deploy**.

   De forma predeterminada, solo la función de administrador tiene privilegios para usar el servicio vSphere Auto Deploy.

2 En la página **Auto Deploy**, seleccione la instancia de vCenter Server en el menú desplegable en la parte superior.

3 Haga clic en **Habilitar Auto Deploy e Image Builder** para activar el servicio.

   Si el servicio de **Image Builder** ya está activo, seleccione la pestaña **Configurar** y haga clic en **Habilitar servicio de Auto Deploy**.

   Aparecerá la página **Almacén de software**.

4 Configure el servidor TFTP.

   a Haga clic en la pestaña **Configurar**.

   b Haga clic en **Descargar ZIP de arranque TFTP** para descargar el archivo de configuración de TFTP y, a continuación, descomprima el archivo en el directorio en el que el servidor TFTP almacena los archivos.

   c (opcional) Para utilizar un servidor proxy, haga clic en **Agregar** en el panel *Resumen de tiempo de ejecución de Auto Deploy* e introduzca una dirección URL del servidor proxy en el cuadro de texto.

      Mediante el proxy inverso, los servidores pueden descargar las solicitudes realizadas al servidor vSphere Auto Deploy.

5 Configure el servidor DHCP de manera que apunte al servidor TFTP en el que se encuentra el archivo ZIP de TFTP.

   a Especifique la dirección IP del servidor TFTP en la opción 66 del DHCP, la cual se suele llamar next-server.

   b Especifique el nombre de archivo de arranque, que es `snponly64.efi.vmw-hardwired` para UEFI o `undionly.kpxe.vmw-hardwired` para BIOS, en la opción 67 de DHCP, a menudo denominado `boot-filename`.

6 Configure todos los hosts que desea aprovisionar con vSphere Auto Deploy para realizar un arranque de red o un arranque PXE, según las instrucciones del fabricante.

7 (opcional) Si configura el entorno de manera que se utilice el modo de huellas digitales, puede reemplazar el certificado `rbd-ca.crt` de OpenSSL y la clave privada `rbd-ca.key` de OpenSSL por un certificado y una clave privada personales para utilizar su propia entidad de certificación (Certificate Authority, CA).

   Los archivos se encuentran en `/etc/vmware-rbd/ssl/`.

   De forma predeterminada, vCenter Server usa VMware Certificate Authority (VMCA).

Resultados

Cuando inicia un host ESXi que está configurado para vSphere Auto Deploy, el host se comunica con el servidor DHCP y se redirige al servidor vSphere Auto Deploy, el cual aprovisiona el host con el perfil de imagen especificado en el conjunto de reglas activas.

Pasos siguientes

- Puede cambiar las propiedades de configuración predeterminadas del **Servicio Auto Deploy**. Para obtener más información, consulte "Configurar vCenter Server" en la documentación de *Administrar vCenter Server y hosts*.
- Puede cambiar las propiedades de configuración predeterminadas del **Servicio Image Builder**. Para obtener más información, consulte "Configurar vCenter Server" en la documentación de *Administrar vCenter Server y hosts*.
- Defina una regla que asigne un perfil de imagen y un perfil de host opcional, ubicación de host o paquete de scripts al host. Para administrar vSphere Auto Deploy con cmdlets de PowerCLI, consulte la sección Administrar vSphere Auto Deploy con cmdlets de PowerCLI. Para administrar vSphere Auto Deploy con vSphere Client, consulte la sección Administrar vSphere Auto Deploy con vSphere Client.
- (opcional) Configure el primer host que aprovisione como un host de referencia. Utilice el almacenamiento y la red, entre otras opciones que desea que el host de destino comparta. Cree un perfil de host para el host de referencia y escriba una regla que asigne tanto el perfil de imagen que ya se ha probado como el perfil de host a los hosts de destino.

- (opcional) Si desea que vSphere Auto Deploy sobrescriba las particiones existentes, configure un host de referencia de manera que realice la partición de forma automática y, a continuación, aplique el perfil de host del host de referencia a otros hosts. Consulte Configurar un host de referencia para la creación automática de particiones .
- (opcional) Si debe configurar información específica de un host, configure el perfil de host del host de referencia de manera que solicite la interacción del usuario. Para obtener más información sobre la personalización de host, consulte la documentación *Perfiles de host de vSphere*.

Usar los cmdlets de vSphere Auto Deploy

Los cmdlets de vSphere Auto Deploy se implementan como cmdlets de Microsoft PowerShell y se incluyen en PowerCLI. Los usuarios de los cmdlets de vSphere Auto Deploy pueden aprovechar todas las funciones de PowerCLI.

Los usuarios experimentados de PowerShell también pueden utilizar los cmdlets de vSphere Auto Deploy del mismo modo que los cmdlets de PowerShell. Si no está familiarizado con PowerShell y PowerCLI, las sugerencias siguientes pueden ser de utilidad.

Puede escribir cmdlets, parámetros y valores de parámetros en el shell de PowerCLI.

- Obtenga ayuda para cualquier cmdlet a través de `Get-Help`*`cmdlet_name`*.
- Recuerde que PowerShell no distingue mayúsculas de minúsculas.
- Utilice la opción de finalización con tabulación para los nombres de cmdlets y parámetros.
- Puede aplicar formato a cualquier resultado de cmdlet o variable mediante `Format-List` o `Format-Table`, o mediante sus formas abreviadas: `fl` o `ft`. Para obtener más información, ejecute el cmdlet `Get-Help Format-List`.

Transmitir parámetros por nombre

Puede transmitir parámetros por nombre en la mayoría de los casos y rodear los valores de parámetros que contienen espacios o caracteres especiales con comillas dobles.

```
Copy-DeployRule -DeployRule testrule -ReplaceItem MyNewProfile
```

La mayoría de los ejemplos de la documentación *Instalar y configurar vCenter Server* transmiten parámetros por nombre.

Transmitir parámetros como objetos

Puede transmitir parámetros como objetos si desea ejecutar scripts y automatización. Transmitir parámetros como objetos resulta útil con los cmdlets que devuelven varios objetos y con los cmdlets que devuelven un solo objeto. Tenga en cuenta el ejemplo siguiente:

1 Vincule a una variable el objeto que contiene la información de cumplimiento de normas de un conjunto de reglas para un host.

   ```
   $tr = Test-DeployRuleSetCompliance MyEsxi42
   ```

2 Vea la propiedad `itemlist` del objeto para determinar la diferencia entre lo que contiene el conjunto de reglas y lo que usa el host actualmente.

```
$tr.itemlist
```

3 Corrija el host para que use el conjunto de reglas modificado, utilizando el cmdlet `Repair-DeployRuleSetCompliance` con la variable.

```
Repair-DeployRuleSetCompliance $tr
```

En este ejemplo, se corrige el host la próxima vez que se arranca.

Configurar licencias masivas

Puede utilizar vSphere Client o ESXi Shell para especificar claves de licencia individuales o configurar licencias masivas mediante los cmdlets de PowerCLI. Las licencias masivas funcionan para todos los hosts ESXi, pero son especialmente útiles para los hosts aprovisionados con vSphere Auto Deploy.

La asignación de claves de licencia mediante vSphere Client y la asignación de licencias mediante los cmdlets de PowerCLI funcionan de manera diferente.

Asignación de claves de licencia mediante vSphere Client

Puede asignar claves de licencia a un host al agregar el host al sistema vCenter Server o cuando un sistema vCenter Server administra el host.

Asignar claves de licencia mediante LicenseDataManager PowerCLI

Puede especificar un conjunto de claves de licencia para agregar a un conjunto de hosts. Las claves de licencia se agregan a la base de datos de vCenter Server. Cada vez que se agrega un host al sistema vCenter Server o vuelve a conectarse a él, se le asigna una clave de licencia. Una clave de licencia que se asigna mediante PowerCLI se trata como una clave de licencia predeterminada. Cuando se agrega o se vuelve a conectar un host sin licencia, se le asigna la clave de licencia predeterminada. Si un host ya tiene licencia, mantiene su clave de licencia.

En el ejemplo siguiente, se asignan licencias a todos los hosts de un centro de datos. También puede asociar licencias con hosts y clústeres.

El ejemplo siguiente está destinado a usuarios avanzados de PowerCLI que saben cómo usar variables de PowerShell.

Requisitos previos

Preparar el sistema para vSphere Auto Deploy.

Procedimiento

1 En una sesión de PowerCLI, conéctese al sistema vCenter Server que desea utilizar y vincule el administrador de licencias asociado a una variable.

```
Connect-VIServer -Server 192.XXX.X.XX -User username -Password password
$licenseDataManager = Get-LicenseDataManager
```

2 Ejecute un cmdlet que recupere el centro de datos donde se encuentran los hosts para los cuales desea utilizar la función de licencias masivas.

```
$hostContainer = Get-Datacenter -Name Datacenter-X
```

También puede ejecutar un cmdlet que recupere un clúster con la finalidad de utilizar licencias masivas para todos los hosts de un clúster, o que recupere una carpeta con la finalidad de utilizar licencias masivas para todos los hosts de una carpeta.

3 Cree un objeto `LicenseData` y un objeto `LicenseKeyEntry` con la clave de licencia y el identificador de tipo asociados.

```
$licenseData = New-Object VMware.VimAutomation.License.Types.LicenseData
$licenseKeyEntry = New-Object Vmware.VimAutomation.License.Types.LicenseKeyEntry
$licenseKeyEntry.TypeId = "vmware-vsphere"
$licenseKeyEntry.LicenseKey = "XXXXX-XXXXX-XXXXX-XXXXX-XXXXX"
```

4 Asocie el atributo `LicenseKeys` del objeto `LicenseData` que creó en el paso 3 con el objeto `LicenseKeyEntry`.

```
$licenseData.LicenseKeys += $licenseKeyEntry
```

5 Actualice los datos de licencias del centro de datos con el objeto `LicenseData` y compruebe que la licencia esté asociada con el contenedor de host.

```
$licenseDataManager.UpdateAssociatedLicenseData($hostContainer.Uid, $licenseData)
$licenseDataManager.QueryAssociatedLicenseData($hostContainer.Uid)
```

6 Aprovisione un host o más con vSphere Auto Deploy y asígnelos al centro de datos o al clúster al que asignó los datos de licencias.

7 Puede usar vSphere Client para verificar que el host se haya asignado correctamente a la licencia predeterminada `XXXXX-XXXXX-XXXXX-XXXXX-XXXXX`.

Resultados

Todos los hosts que se hayan asignado al centro de datos ahora cuentan con licencia de manera automática.

Cómo funciona vSphere Auto Deploy con PowerCLI

Puede administrar vSphere Auto Deploy con cmdlets de PowerCLI para crear reglas que asocien hosts ESXi con varios objetos en la instancia de destino de vCenter.

Puede administrar vSphere Auto Deploy con cmdlets de PowerCLI para crear reglas que asocien hosts con perfiles de imagen, perfiles de host, scripts personalizados y ubicaciones en la instancia de destino de vCenter Server. También es posible actualizar los hosts mediante la comprobación del cumplimiento de normas y la corrección de los problemas de cumplimiento de normas que correspondan.

Administrar vSphere Auto Deploy con cmdlets de PowerCLI

Puede administrar vSphere Auto Deploy con cmdlets de PowerCLI para crear reglas que asocien hosts con perfiles de imagen, perfiles de host, scripts personalizados y ubicaciones en la instancia de vCenter Server de destino. También es posible actualizar los hosts mediante la comprobación del cumplimiento de normas y la corrección de los problemas de cumplimiento de normas que correspondan.

Introducción al proceso de vSphere Auto Deploy con PowerCLI

Para comenzar a usar vSphere Auto Deploy, debe aprender cómo funciona vSphere Auto Deploy, instalar el servidor vSphere Auto Deploy, instalar PowerCLI, escribir reglas de PowerCLI que aprovisionen hosts y encender los hosts que deben arrancarse con el perfil de imagen especificado. Puede personalizar el perfil de imagen, el perfil de host y la ubicación de vCenter Server.

Consulte Escenario de vSphere PowerCLI para vSphere Auto Deploy para obtener un ejercicio paso a paso que lo ayude a configurar su primer entorno de vSphere Auto Deploy.

Para aprovisionar correctamente los hosts en su entorno con vSphere Auto Deploy, puede seguir estos pasos.

1 Implementar vCenter Server.

   Se incluye el servidor vSphere Auto Deploy.

2 Configure el tipo de inicio para el servicio de vSphere Auto Deploy.

   Consulte Preparar el sistema para vSphere Auto Deploy.

3 Instale PowerCLI, que incluye cmdlets de vSphere Auto Deploy y vSphere ESXi Image Builder.

   Consulte Configurar vSphere ESXi Image Builder , Usar los cmdlets de vSphere Auto Deploy y Usar cmdlets de VMware.Image Builder .

4 Busque el perfil de imagen que incluye los VIB que desea implementar en los hosts.

   - A menudo, deberá agregar los almacenes que contienen el software necesario a la sesión de PowerCLI y, a continuación, seleccionar un perfil de imagen desde uno de esos almacenes.
   - Si desea crear un perfil de imagen personalizado, use los cmdlets de vSphere ESXi Image Builder para clonar un perfil de imagen existente y agregue los VIB personalizados al clon. Agregue el perfil de imagen personalizado a la sesión de PowerCLI.

Debe utilizar vSphere ESXi Image Builder para la personalización solamente si tiene que agregar o quitar VIB. En la mayoría de los casos, puede agregar el almacén en el que VMware aloja los perfiles de imagen a la sesión de PowerCLI como una URL.

5 Inicie una sesión de PowerCLI y conéctese con el sistema vCenter Server con el que vSphere Auto Deploy está registrado.

6 Use el cmdlet `New-DeployRule` de PowerCLI para escribir una regla que asigne el perfil de imagen a un host, a varios hosts especificados mediante un patrón o a todos los hosts.

```
New-DeployRule -Name "testrule" -Item perfil-imagen -AllHosts
```

Consulte Asignar un perfil de imagen a hosts.

Nota vSphere Auto Deploy se optimizó para aprovisionar hosts que contienen una dirección MAC fija a una asignación de dirección IP en DHCP (a veces se denominan reservas de DHCP). Si desea utilizar direcciones IP estáticas, debe configurar el perfil de host para que solicite la personalización del host. Para obtener más información, consulte la documentación sobre *Perfiles de host de vSphere*.

---

7 Encienda los hosts que desea aprovisionar.

8 Configure el host aprovisionado como host de referencia para el perfil de host.

Puede especificar la configuración de Syslog del host de referencia, la configuración del firewall, el almacenamiento, las redes, etc.

9 Configure el host aprovisionado como host de referencia para el perfil de host.

Puede especificar la configuración de Syslog del host de referencia, la configuración del firewall, el almacenamiento, las redes, etc. Consulte Configurar un host de referencia de vSphere Auto Deploy.

10 Cree y exporte un perfil de host para el host de referencia.

Consulte la documentación sobre *perfiles de host*.

11 Para aprovisionar varios hosts con el perfil de host, use el cmdlet `Copy-DeployRule` para editar la regla creada anteriormente.

Puede revisar la regla para asignar no solo un perfil de imagen, sino también un perfil de host, una ubicación de vCenter Server y un paquete de scripts personalizado.

```
Copy-DeployRule -DeployRule "testrule" -ReplaceItem
mi_perfil_de_host_de_referencia,mi_clúster_de_destino
              -ReplacePattern  "ipv4=192.XXX.1.10-192.XXX.1.20"
```

Donde *mi_perfil_de_host_de_referencia* es el nombre del perfil de host de referencia y *mi_clúster_de_destino* es el nombre del clúster de destino.

12 Realice las operaciones de cumplimiento de prueba y reparación para corregir los hosts.

Consulte Probar y reparar cumplimiento de reglas .

13 Compruebe que los hosts aprovisionados cumplan los siguientes requisitos:

- Cada host está conectado al sistema vCenter Server.
- Los hosts no están en modo de mantenimiento.
- Los hosts no presentan instancias de incumplimiento de normas.
- Cada host con un perfil de host que requiere entradas del usuario tiene información actualizada de personalización del host.

Corrija los problemas de cumplimiento y asociaciones de hosts, y reinicie los hosts hasta que todos los hosts cumplan con los requisitos.

Consulte para obtener una introducción al proceso de arranque, las diferencias entre el primer arranque y los arranques posteriores y una descripción general del uso de la personalización de hosts.

Usar los cmdlets de vSphere Auto Deploy

Los cmdlets de vSphere Auto Deploy se implementan como cmdlets de Microsoft PowerShell y se incluyen en PowerCLI. Los usuarios de los cmdlets de vSphere Auto Deploy pueden aprovechar todas las funciones de PowerCLI.

Los usuarios experimentados de PowerShell también pueden utilizar los cmdlets de vSphere Auto Deploy del mismo modo que los cmdlets de PowerShell. Si no está familiarizado con PowerShell y PowerCLI, las sugerencias siguientes pueden ser de utilidad.

Puede escribir cmdlets, parámetros y valores de parámetros en el shell de PowerCLI.

- Obtenga ayuda para cualquier cmdlet a través de `Get-Help`*`cmdlet_name`*.
- Recuerde que PowerShell no distingue mayúsculas de minúsculas.
- Utilice la opción de finalización con tabulación para los nombres de cmdlets y parámetros.
- Puede aplicar formato a cualquier resultado de cmdlet o variable mediante `Format-List` o `Format-Table`, o mediante sus formas abreviadas: `fl` o `ft`. Para obtener más información, ejecute el cmdlet `Get-Help Format-List`.

Transmitir parámetros por nombre

Puede transmitir parámetros por nombre en la mayoría de los casos y rodear los valores de parámetros que contienen espacios o caracteres especiales con comillas dobles.

```
Copy-DeployRule -DeployRule testrule -ReplaceItem MyNewProfile
```

La mayoría de los ejemplos de la documentación *Instalar y configurar vCenter Server* transmiten parámetros por nombre.

Transmitir parámetros como objetos

Puede transmitir parámetros como objetos si desea ejecutar scripts y automatización. Transmitir parámetros como objetos resulta útil con los cmdlets que devuelven varios objetos y con los cmdlets que devuelven un solo objeto. Tenga en cuenta el ejemplo siguiente:

1 Vincule a una variable el objeto que contiene la información de cumplimiento de normas de un conjunto de reglas para un host.

```
$tr = Test-DeployRuleSetCompliance MyEsxi42
```

2 Vea la propiedad `itemlist` del objeto para determinar la diferencia entre lo que contiene el conjunto de reglas y lo que usa el host actualmente.

```
$tr.itemlist
```

3 Corrija el host para que use el conjunto de reglas modificado, utilizando el cmdlet `Repair-DeployRuleSetCompliance` con la variable.

```
Repair-DeployRuleSetCompliance $tr
```

En este ejemplo, se corrige el host la próxima vez que se arranca.

Descripción general de cmdlets de vSphere Auto Deploy PowerCLI

El usuario especifica las reglas que asignan perfiles de imagen y perfiles de host a los hosts mediante un conjunto de cmdlets de PowerCLI que se incluyen en PowerCLI.

Si no está familiarizado con PowerCLI, lea la documentación de PowerCLI y consulte Usar los cmdlets de vSphere Auto Deploy. Puede obtener ayuda en relación con cualquier comando en la línea de comandos de PowerShell.

- Ayuda básica: `Get-Help` *nombre_del_cmdlet*
- Ayuda detallada: `Get-Help` *nombre_del_cmdlet* `-Detailed`

Nota Al ejecutar cmdlets de vSphere Auto Deploy, proporcione todos los parámetros en la línea de comandos cuando invoque el cmdlet. No se recomienda proporcionar parámetros en modo interactivo.

Tabla 4-18. Cmdlets de PowerCLI del motor de reglas

Comando	Descripción
`Get-DeployCommand`	Devuelve una lista de cmdlets de vSphere Auto Deploy.
`New-DeployRule`	Crea una nueva regla con los elementos y los patrones especificados.
`Set-DeployRule`	Actualiza una regla existente con los elementos y los patrones especificados. No es posible actualizar una regla que forma parte de un conjunto de reglas.
`Get-DeployRule`	Recupera las reglas con los nombres especificados.

Tabla 4-18. Cmdlets de PowerCLI del motor de reglas (continuación)

Comando	Descripción
`Copy-DeployRule`	Clona y actualiza una regla existente.
`Add-DeployRule`	Agrega una regla o más al conjunto de reglas de trabajo y, de forma predeterminada, también al conjunto de reglas activo. Utilice el parámetro `NoActivate` para agregar una regla solamente al conjunto de reglas de trabajo.
`Remove-DeployRule`	Elimina una regla o más del conjunto de reglas de trabajo y del conjunto de reglas activo. Ejecute este comando con el parámetro `-Delete` para eliminar la regla por completo.
`Set-DeployRuleset`	Establece de manera explícita la lista de reglas en el conjunto de reglas de trabajo.
`Get-DeployRuleset`	Recupera el conjunto de reglas de trabajo o el conjunto de reglas activo actuales.
`Switch-ActiveDeployRuleset`	Activa un conjunto de reglas para que todas las solicitudes nuevas se evalúen mediante el conjunto de reglas.
`Get-VMHostMatchingRules`	Recupera las reglas que coinciden con un patrón. Por ejemplo, es posible recuperar todas las reglas que se aplican a un host o a varios. Utilice este cmdlet principalmente para depuración.
`Test-DeployRulesetCompliance`	Comprueba si los elementos asociados con un host especificado cumplen los criterios del conjunto de reglas activo.
`Repair-DeployRulesetCompliance`	En función del resultado de `Test-DeployRulesetCompliance`, este cmdlet actualiza el perfil de imagen, el perfil de host y la ubicación de cada host en el inventario de vCenter Server. El cmdlet puede aplicar perfiles de imagen, aplicar perfiles de host o transferir hosts a carpetas o clústeres especificados previamente en el sistema vCenter Server.
`Apply-EsxImageProfile`	Asocia el perfil de imagen especificado con el host especificado.
`Get-VMHostImageProfile`	Recupera el perfil de imagen que utiliza un host especificado. Este cmdlet es diferente al cmdlet `Get-EsxImageProfile` en vSphere ESXi Image Builder.
`Repair-DeployImageCache`	Utilice este cmdlet solamente si la memoria caché de imagen de vSphere Auto Deploy se elimina por accidente.
`Get-VMHostAttributes`	Recupera los atributos de un host que se utilizan cuando el servidor vSphere Auto Deploy evalúa las reglas.
`Get-DeployMachineIdentity`	Devuelve un valor de cadena que vSphere Auto Deploy utiliza para vincular forma lógica un host ESXi de vCenter Server con una máquina física.
`Set-DeployMachineIdentity`	Vincula de forma lógica un objeto de host en la base de datos de vCenter Server con una máquina física. Utilice este cmdlet para agregar hosts sin especificar reglas.

Tabla 4-18. Cmdlets de PowerCLI del motor de reglas (continuación)

Comando	Descripción
`Get-DeployOption`	Recupera las opciones de configuración globales de vSphere Auto Deploy. Actualmente, este cmdlet es compatible con la opción `vlan-id`, la cual especifica el identificador de VLAN predeterminado para la red de administración de ESXi de un host aprovisionado con vSphere Auto Deploy. vSphere Auto Deploy utiliza el valor solo si el host se arranca sin un perfil de host.
`Set-DeployOption`	Establece el valor de una opción de configuración global. Actualmente, es compatible con la opción `vlan-id` para establecer un identificador de la VLAN predeterminado para la red de administración de ESXi.
`Add-ProxyServer`	Agrega un servidor proxy a la base de datos de vSphere Auto Deploy. Ejecute el comando con el parámetro `-Address` para especificar la dirección IPv4 o IPv6. La dirección puede incluir un número de puerto.
`List-ProxyServer`	Lista los servidores proxy que están registrados actualmente en vSphere Auto Deploy.
`Delete-ProxyServer`	Elimina uno o varios servidores proxy de la lista de los servidores proxy registrados en vSphere Auto Deploy. Puede ejecutar el comando con el parámetro `-id` desde la lista de servidores proxy o con el parámetro `-Address` especificando la dirección IPv4 o IPv6 del servidor proxy que desea eliminar.
`Add-ScriptBundle`	Agrega uno o varios paquetes de scripts al servidor vSphere Auto Deploy.
`Get-ScriptBundle`	Recupera la lista de paquetes de scripts disponible en el servidor vSphere Auto Deploy, así como los scripts que contiene.
`Remove-ScriptBundle`	Elimina un paquete de scripts de vSphere Auto Deploy. Aplicable para la versión 6.7 y versiones posteriores de vSphere.
`Get-CustomCertificate`	Recupera el certificado de host personalizado cargado en AutoDeploy. Debe ejecutar el comando con el parámetro `-HostId [MAC_Address | BIOS_UUID]`. La primera vez que agregue certificados personalizados, no verá ningún certificado devuelto mediante este cmdlet.
`List-CustomCertificates`	Recupera información sobre todos los certificados de host personalizados utilizados por Auto Deploy. La lista proporciona detalles del nombre del certificado, `Host ID` y `Associated Host Name`, lo cual refleja el nombre de la instancia de vCenter Server para el servidor Auto Deploy.

Tabla 4-18. Cmdlets de PowerCLI del motor de reglas (continuación)

Comando	Descripción
`Add-CustomCertificate`	Agrega un certificado personalizado al almacén de certificados de endpoints de VMware y lo asocia con un host ESXi. El certificado se activa al reiniciar el host. Puede utilizar el cmdlet `Get-CustomCertificate` para recuperar la clave del certificado de host personalizada. Puede ejecutar el comando con el parámetro `-HostId [MAC_Address | BIOS_UUID]` para asociar el certificado al host al especificar un `-Key [file:///path/to/key.key]` y `-Cert [file:///path/to/cert.crt]`. El uso de este cmdlet requiere el privilegio **AutoDeploy.Rule.Create** en la carpeta raíz de vCenter Server.
`Remove-CustomCertificate`	Elimina un conjunto de certificados de host personalizados de Auto Deploy. Las entradas de certificado se eliminan de la base de datos y los archivos de certificado se eliminan del almacén de archivos. Es necesario reiniciar los hosts que ya se hayan arrancado con un certificado personalizado para poder recibir un certificado nuevo. Debe proporcionar al menos uno de los parámetros `-Cert` o `-HostId`. El uso de este cmdlet requiere el privilegio **AutoDeploy.Rule.Create** en la carpeta raíz de vCenter Server.

Asignar un perfil de imagen a hosts

Antes de que pueda aprovisionar un host, deberá crear reglas que asignen un perfil de imagen a cada host que desee aprovisionar con vSphere Auto Deploy.

Las reglas de extensibilidad de vSphere Auto Deploy obligan a que los VIB en el nivel CommunitySupported solo puedan contener archivos de determinadas ubicaciones predefinidas, como la ruta de complementos de ESXCLI, la ruta de complementos de jumpstart, etc. Si agrega un VIB que se encuentra en una ubicación diferente de la de un perfil de imagen, aparecerá una advertencia. Puede anular la advertencia utilizando la opción `force` (forzar).

Si realiza una llamada al cmdlet `New-DeployRule` en un perfil de imagen que incluye VIB en el nivel CommunitySupported que infrinja la regla, establezca `$DeployNoSignatureCheck = $true` antes de agregar el perfil de imagen. Con esta configuración, el sistema omitirá la validación de firma y no realizará la comprobación de reglas de extensibilidad.

Nota Los perfiles de imagen que incluyen VIB en el nivel CommunitySupported no se admiten en los sistemas de producción.

Procedimiento

1 En una sesión de PowerCLI, ejecute el cmdlet `Connect-VIServer` para conectarse al sistema vCenter Server con el que se registró vSphere Auto Deploy.

```
Connect-VIServer ipv4_or_ipv6_address
```

Es posible que el cmdlet devuelva una advertencia de certificado de servidor. En un entorno de producción, asegúrese de que no se emita ninguna advertencia de certificado de servidor. En un entorno de desarrollo, puede omitir la advertencia.

2 Determine la ubicación del almacén de software público o defina un perfil de imagen personalizado con vSphere ESXi Image Builder.

3 Ejecute `Add-EsxSoftwareDepot` para agregar el almacén de software que contiene el perfil de imagen a la sesión de PowerCLI.

Tipo de almacén	Cmdlet
Almacén remoto	Ejecute **`Add-EsxSoftwareDepot`** ***`url_del_almacén`***.
Archivo ZIP	a Descargue el archivo ZIP en la ruta de acceso de archivo local. b Ejecute **`Add-EsxSoftwareDepot C:\file_path\my_offline_depot.zip`**.

4 En el almacén, busque el perfil de imagen que desea utilizar ejecutando el cmdlet `Get-EsxImageProfile`.

De manera predeterminada, el almacén de ESXi incluye un perfil de imagen base que incluye VMware Tools y tiene la cadena `standard` en su nombre y un perfil de imagen base que no incluye VMware Tools.

5 Defina una regla en la que los hosts con determinados atributos, por ejemplo un rango de direcciones IP, estén asignados al perfil de imagen.

```
New-DeployRule -Name "testrule" -Item "My Profile25" -Pattern "vendor=Acme,Zven",
"ipv4=192.XXX.1.10-192.XXX.1.20"
```

Si un nombre contiene espacios, se requieren comillas dobles. De lo contrario, es opcional. Especifique `-AllHosts` en lugar de un patrón para aplicar el elemento a todos los hosts.

El cmdlet crea una regla con el nombre `testrule`. La regla asigna el perfil de imagen con el nombre My Profile25 a todos los hosts con un proveedor de Acme o Zven que también tienen una dirección IP en el rango especificado.

6 Agregue la regla al conjunto de reglas.

```
Add-DeployRule testrule
```

De manera predeterminada, la regla se agrega al conjunto de reglas en funcionamiento y al conjunto de reglas activo. Si utiliza el parámetro `NoActivate`, el conjunto de reglas en funcionamiento no se convierte en el conjunto de reglas activo.

Resultados

Cuando el host arranca desde iPXE, informa de los atributos de la máquina a la consola. Utilice el mismo formato de los atributos al escribir reglas de implementación.

```
*****************************************************************
* Booting through VMware AutoDeploy...
*
* Machine attributes:
* . asset=No Asset Tag
* . domain=vmware.com
* . hostname=myhost.mycompany.com
* . ipv4=XX.XX.XXX.XXX
* . mac=XX:Xa:Xb:Xc:Xx:XX
* . model=MyVendorModel
* . oemstring=Product ID: XXXXXX-XXX
* . serial=XX XX XX XX XX XX...
* . uuid=XXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXX
* . vendor=MyVendor
*****************************************************************
```

Pasos siguientes

- Para los hosts que ya se han aprovisionado con vSphere Auto Deploy, realice la prueba de cumplimiento de normas y las operaciones de reparación con la finalidad de aprovisionarlos con el nuevo perfil de imagen. Consulte Probar y reparar cumplimiento de reglas .
- Encienda los hosts no aprovisionados para aprovisionarlos con el nuevo perfil de imagen.

Escribir una regla y asignar un perfil de host a hosts

vSphere Auto Deploy puede asignar un perfil de host a uno o más hosts ESXi.

En muchos casos, puede asignar un host a un clúster en lugar de especificar un perfil de host explícitamente. El host utiliza el perfil de host del clúster.

Requisitos previos

El perfil de host puede incluir información sobre la configuración de almacenamiento, la configuración de red u otras características del host. Si agrega un host a un clúster, se utiliza el perfil de host de ese clúster.

- Instale PowerCLI y todo el software de requisito previo. Para obtener información, consulte Instalar y configurar vCenter Server.
- Exporte el perfil de host que desea utilizar.

Procedimiento

1 En una sesión de PowerCLI, ejecute el cmdlet `Connect-VIServer` para conectarse al sistema vCenter Server con el que se registró vSphere Auto Deploy.

```
Connect-VIServer ipv4_or_ipv6_address
```

Es posible que el cmdlet devuelva una advertencia de certificado de servidor. En un entorno de producción, asegúrese de que no se emita ninguna advertencia de certificado de servidor. En un entorno de desarrollo, puede omitir la advertencia.

2 Con vSphere Client, configure un host con los parámetros que desee usar y cree un perfil de host a partir de él.

3 Busque el nombre del perfil de host mediante la ejecución del cmdlet `Get-VMhostProfile` de PowerCLI, pasando el host ESXi a partir del cual creó un perfil de host.

4 En el símbolo de PowerCLI, defina una regla en la que los perfiles de host se asignen a hosts con ciertos atributos; por ejemplo, un intervalo de direcciones IP.

```
New-DeployRule -Name "testrule2" -Item my_host_profile -Pattern "vendor=Acme,Zven",
"ipv4=192.XXX.1.10-192.XXX.1.20"
```

El elemento especificado se asigna a todos los hosts que posean los atributos especificados. Este ejemplo especifica una regla denominada testrule2. Esta asigna el perfil de host especificado *mi_perfil_de_host* a todos los hosts que tengan una dirección IP dentro del intervalo especificado y cuyo fabricante sea Acme o Zven.

5 Agregue la regla al conjunto de reglas.

```
Add-DeployRule testrule2
```

De forma predeterminada, el conjunto de reglas en funcionamiento se convierte en el conjunto de reglas activo y los cambios en él se vuelven activos cuando agrega una regla. Si utiliza el parámetro `NoActivate`, el conjunto de reglas en funcionamiento no se convierte en el conjunto de reglas activo.

Pasos siguientes

- Asigne un host ya aprovisionado con vSphere Auto Deploy al nuevo perfil de host. Para ello, realice operaciones de prueba de cumplimiento y reparación en esos hosts. Para obtener más información, consulte Probar y reparar cumplimiento de reglas .
- Encienda los hosts no aprovisionados para aprovisionarlos con el perfil de host.

Escribir una regla y asignar un host a una carpeta o un clúster

vSphere Auto Deploy puede asignar un host a una carpeta o un clúster. Cuando el host arranca, vSphere Auto Deploy lo agrega a la ubicación que se especifica en vCenter Server. El host asignado a un clúster hereda el perfil de host del clúster.

Requisitos previos

- Prepare el sistema e instale el servidor Auto Deploy. Para obtener más información, consulte Preparar el sistema para vSphere Auto Deploy.
- Compruebe que la carpeta seleccionada esté en un centro de datos o clúster. No puede asignar el host a una carpeta de nivel superior independiente.

Procedimiento

1 En una sesión de PowerCLI, ejecute el cmdlet `Connect-VIServer` para conectarse al sistema vCenter Server con el que se registró vSphere Auto Deploy.

```
Connect-VIServer ipv4_or_ipv6_address
```

Es posible que el cmdlet devuelva una advertencia de certificado de servidor. En un entorno de producción, asegúrese de que no se emita ninguna advertencia de certificado de servidor. En un entorno de desarrollo, puede omitir la advertencia.

2 Defina una regla en la que los hosts con ciertos atributos, por ejemplo, un rango de direcciones IP, se asignan a una carpeta o un clúster.

```
New-DeployRule -Name testrule3 -Item "mi carpeta"    -Pattern "vendor=Acme,Zven",
"ipv4=192.XXX.1.10-192.XXX.1.20"
```

Este ejemplo pasa la carpeta por el nombre. En cambio, puede pasar una carpeta, un clúster o un objeto de centro de datos que recupere con el comando cmdlet `Get-Folder`, `Get-Cluster` o `Get-Datacenter`.

3 Agregue la regla al conjunto de reglas.

```
Add-DeployRule testrule3
```

De forma predeterminada, el conjunto de reglas en funcionamiento se convierte en el conjunto de reglas activo y los cambios en él se vuelven activos cuando agrega una regla. Si utiliza el parámetro `NoActivate`, el conjunto de reglas en funcionamiento no se convierte en el conjunto de reglas activo.

Pasos siguientes

- Para asignar un host ya aprovisionado con vSphere Auto Deploy a la nueva ubicación de carpeta o clúster, realice una operación de cumplimiento de prueba y reparación. Consulte Probar y reparar cumplimiento de reglas .
- Encienda los hosts no aprovisionados para agregarlos a la ubicación especificada de vCenter Server.

Configurar un sistema sin estado mediante la ejecución de un script personalizado

Puede utilizar vSphere Auto Deploy para configurar uno o varios hosts asociando scripts personalizados con una regla de vSphere Auto Deploy.

Los scripts se ejecutan en orden alfabético después del flujo de trabajo de arranque de ESXi del host.inicial del host.

Requisitos previos

- Compruebe que el paquete de scripts que desea asociar a la regla de vSphere Auto Deploy tiene el formato `.tgz` y un tamaño máximo de 10 MB, y que está escrito en lenguaje de script de ash de BusyBox o Python.

Procedimiento

1 En una sesión de PowerCLI, ejecute el cmdlet `Connect-VIServer` para conectarse al sistema vCenter Server con el que se registró vSphere Auto Deploy.

```
Connect-VIServer ipv4_or_ipv6_address
```

Es posible que el cmdlet devuelva una advertencia de certificado de servidor. En un entorno de producción, asegúrese de que no se emita ninguna advertencia de certificado de servidor. En un entorno de desarrollo, puede omitir la advertencia.

2 Ejecute el cmdlet `Add-ScriptBundle` para agregar el paquete de scripts que contiene los scripts necesarios al inventario de vSphere Auto Deploy.

```
Add-ScriptBundle c:/temp/MyScriptBundle.tgz
```

El nombre del paquete de scripts sin la extensión `.tgz` es el identificador del nombre o el objeto del elemento del paquete de scripts. Puede actualizar el paquete de scripts existente utilizando el parámetro `-Update` con el cmdlet `Add-ScriptBundle`.

3 (opcional) Ejecute el cmdlet `Get-ScriptBundle` para comprobar que el paquete de scripts se agregó al inventario de vSphere Auto Deploy.

4 Defina una regla en la que los hosts con determinados atributos, por ejemplo un rango de direcciones IP, estén asignados al paquete de scripts.

```
New-DeployRule -Name "testrule4" -Item "MyScriptBundle" -Pattern "vendor=Acme,Zven",
"ipv4=192.XXX.1.10-192.XXX.1.20"
```

Si un nombre contiene espacios, se requieren comillas dobles. De lo contrario, es opcional. Especifique `-AllHosts` en lugar de un patrón para aplicar el elemento a todos los hosts.

Cree una regla denominada *testrule4*. La regla asigna el paquete de scripts con el nombre My Script Bundle a todos los hosts con un proveedor de Acme o Zven que también tienen una dirección IP en el rango especificado. Puede utilizar el identificador de nombre del paquete de scripts o el objeto que devuelve el cmdlet `Get-ScriptBundle` para identificar el paquete de scripts que quiere asociar a la regla.

5 Agregue la regla al conjunto de reglas.

```
Add-DeployRule testrule4
```

De manera predeterminada, la regla se agrega al conjunto de reglas en funcionamiento y al conjunto de reglas activo. Si utiliza el parámetro `NoActivate`, el conjunto de reglas en funcionamiento no se convierte en el conjunto de reglas activo.

Pasos siguientes

- Para los hosts que ya se han aprovisionado con vSphere Auto Deploy, realice la prueba de cumplimiento de normas y las operaciones de reparación con la finalidad de aprovisionarlos con los nuevos scripts. Consulte Probar y reparar cumplimiento de reglas .
- Encienda los hosts no aprovisionados para aprovisionarlos con los nuevos scripts.

Probar y reparar cumplimiento de reglas

Pruebe el cumplimiento de las reglas nuevas o modificadas y repare según corresponda, ya que los cambios en el conjunto de reglas de vSphere Auto Deploy no se actualizan automáticamente.

Requisitos previos

Cuando se agrega una regla al conjunto de reglas de vSphere Auto Deploy o cuando se modifican una o más reglas, los hosts no se actualizan de manera automática. vSphere Auto Deploy aplica las reglas nuevas únicamente cuando se prueba el cumplimiento de reglas y se realizan las correcciones pertinentes.

- Prepare el sistema e instale el servidor Auto Deploy. Para obtener más información, consulte Preparar el sistema para vSphere Auto Deploy.
- Compruebe que la infraestructura incluya un host ESXi o más aprovisionados con vSphere Auto Deploy y que el host en el que se instaló PowerCLI pueda acceder a esos hosts ESXi.

Procedimiento

1 En una sesión de PowerCLI, ejecute el cmdlet `Connect-VIServer` para conectarse al sistema vCenter Server con el que se registró vSphere Auto Deploy.

```
Connect-VIServer ipv4_or_ipv6_address
```

Es posible que el cmdlet devuelva una advertencia de certificado de servidor. En un entorno de producción, asegúrese de que no se emita ninguna advertencia de certificado de servidor. En un entorno de desarrollo, puede omitir la advertencia.

2 Use PowerCLI para comprobar qué reglas de vSphere Auto Deploy están disponibles actualmente.

```
Get-DeployRule
```

El sistema devuelve las reglas y los patrones, y los elementos asociados.

3 Modifique una de las reglas disponibles.

Por ejemplo, puede cambiar el perfil de imagen y el nombre de la regla.

```
Copy-DeployRule -DeployRule testrule -ReplaceItem MyNewProfile
```

No se puede editar una regla que ya se agregó a un conjunto de reglas activo. En lugar de ello, puede copiar la regla y reemplazar el elemento o el patrón que desea cambiar.

4 Compruebe que pueda acceder al host para el cual desea probar el cumplimiento del conjunto de reglas.

```
Get-VMHost -Name MyEsxi42
```

5 Ejecute el cmdlet que prueba el cumplimiento del conjunto de reglas para el host y vincule el valor devuelto a una variable para usarlo en otro momento.

```
$tr = Test-DeployRuleSetCompliance MyEsxi42
```

6 Examine las diferencias entre el contenido del conjunto de reglas y la configuración del host.

```
$tr.itemlist
```

Si el host para el que desea probar el cumplimiento del nuevo conjunto de reglas cumple con el conjunto de reglas activo, el sistema devuelve una tabla de elementos actuales y esperados.

```

CurrentItem                              ExpectedItem
-----------                              ------------
My Profile 25                            MyNewProfile
```

7 Corrija el host para que use el conjunto de reglas modificado la próxima vez que arranque.

```
Repair-DeployRuleSetCompliance $tr
```

Pasos siguientes

Si la regla que modificó ha especificado la ubicación en el inventario, el cambio se aplica cuando se corrigen los problemas de cumplimiento. Para todos los demás cambios, reinicie el host para que vSphere Auto Deploy aplique la nueva regla y logre el cumplimiento entre el conjunto de reglas y el host.

Registrar la dirección de un servidor proxy de almacenamiento en caché con vSphere Auto Deploy

El arranque simultáneo de un gran número de hosts sin estado supone una carga considerable para el servidor vSphere Auto Deploy. Puede equilibrar la carga de las solicitudes entre el servidor vSphere Auto Deploy y uno o varios servidores proxy más que registre en vSphere Auto Deploy.

Requisitos previos

Procedimiento

1 En una sesión de PowerCLI, ejecute el cmdlet `Connect-VIServer` para conectarse al sistema vCenter Server con el que se registró vSphere Auto Deploy.

```
Connect-VIServer ipv4_or_ipv6_address
```

Es posible que el cmdlet devuelva una advertencia de certificado de servidor. En un entorno de producción, asegúrese de que no se emita ninguna advertencia de certificado de servidor. En un entorno de desarrollo, puede omitir la advertencia.

2 Registre direcciones de un servidor proxy de almacenamiento en caché en vSphere Auto Deploy ejecutando el cmdlet `Add-ProxyServer`.

```
Add-ProxyServer -Address 'https://proxy_server_ip_address:port_number'
```

Puede ejecutar el cmdlet varias veces para registrar varios servidores proxy. La dirección puede incluir un número de puerto.

3 (opcional) Ejecute el cmdlet `List-ProxyServer` para verificar que el servidor proxy de almacenamiento en caché está registrado en vSphere Auto Deploy.

Tareas de vSphere Auto Deploy mediante vSphere Client

Administrar vSphere Auto Deploy con vSphere Client

Puede agregar hosts ESXi al inventario de vSphere Auto Deploy, y crear, supervisar y administrar las reglas, así como las asociaciones de hosts mediante vSphere Client.



(Mejoras de Auto Deploy en vSphere Client)

Introducción al proceso de vSphere Auto Deploy con vSphere Client

Para comenzar a usar vSphere Auto Deploy, debe aprender cómo funciona vSphere Auto Deploy, iniciar los servicios de vCenter Server vSphere ESXi Image Builder y vSphere Auto Deploy, escribir reglas de implementación que aprovisionen hosts y encender los hosts que deben arrancarse con el perfil de imagen especificado.

El flujo de trabajo para aprovisionar los hosts en su entorno con vSphere Auto Deploy incluye las siguientes tareas:

1 Implementar vCenter Server.

   Se incluye el servidor vSphere Auto Deploy.

2 Configure los tipos de inicio de los servicios vSphere Auto Deploy y vSphere ESXi Image Builder.

   Consulte Preparar el sistema para vSphere Auto Deploy y Configurar vSphere ESXi Image Builder.

3 Agregue o importe un almacén de software al inventario de vSphere Auto Deploy.

   Consulte Agregar un almacén de software o Importar un almacén de software.

4 (Opcional) Si quiere crear un perfil de imagen personalizado, clone o cree un perfil de imagen con vSphere Client.

   Consulte Clonar un perfil de imagen o Crear un perfil de imagen.

5 Cree una regla de Auto Deploy que asigne el perfil de imagen a un host, a varios hosts especificados por un patrón o a todos los hosts.

   Consulte Crear una regla de implementación.

   Nota vSphere Auto Deploy se optimizó para aprovisionar hosts que contienen una dirección MAC fija a una asignación de dirección IP en DHCP (a veces se denominan reservas de DHCP). Si desea utilizar direcciones IP estáticas, debe configurar el perfil de host para que solicite la personalización del host. Para obtener más información, consulte la documentación sobre *Perfiles de host de vSphere*.

6 Encienda los hosts que desea aprovisionar.

7 Configure el host aprovisionado como host de referencia para el perfil de host.

   Puede especificar la configuración de Syslog del host de referencia, la configuración del firewall, el almacenamiento, las redes, etc.

8 Extraiga un perfil de host del host de referencia.

   Consulte la documentación sobre *perfiles de host*.

9 Para aprovisionar varios hosts con el perfil de host, clone o edite la regla creada anteriormente con vSphere Client.

   Consulte Clonar una regla de implementación o Editar una regla de Auto Deploy.

10 Active la nueva regla y desactive la anterior.

   Consulte Activar, desactivar y reordenar las reglas de implementación.

11 Corrija las asociaciones de host para aplicar la nueva regla al host.

   Consulte Corregir un host no compatible.

12 Compruebe que los hosts aprovisionados cumplan los siguientes requisitos:

   - Cada host está conectado al sistema vCenter Server.
   - Los hosts no están en modo de mantenimiento.
   - Los hosts no presentan instancias de incumplimiento de normas.
   - Cada host con un perfil de host que requiere entradas del usuario tiene información actualizada de personalización del host.

   Corrija los problemas de cumplimiento y asociaciones de hosts, y reinicie los hosts hasta que todos los hosts cumplan con los requisitos.

Consulte para obtener una introducción al proceso de arranque, las diferencias entre el primer arranque y los arranques posteriores y una descripción general del uso de la personalización de hosts.

Crear una regla de implementación

Antes de aprovisionar los hosts ESXi con vSphere Auto Deploy, debe crear reglas que asignen ubicaciones de host, perfiles de imagen y perfiles de host a los hosts.

Requisitos previos

Un host ESXi puede coincidir con más de un criterio de regla de vSphere Auto Deploy; si eso sucede, se tiene en cuenta el orden de las reglas.

- Prepare el sistema e instale el servidor Auto Deploy. Para obtener más información, consulte Preparar el sistema para vSphere Auto Deploy.
- Si desea incluir un perfil de imagen en la regla, compruebe que se haya agregado el almacén de software necesario al inventario. Consulte Agregar un almacén de software o Importar un almacén de software.

Procedimiento

Procedimiento

1 Desplácese hasta **Inicio > Auto Deploy**.

De forma predeterminada, solo la función de administrador tiene privilegios para usar el servicio vSphere Auto Deploy.

2 En la pestaña **Reglas de implementación**, haga clic en **Nueva regla de implementación**.

Aparece el asistente **Nueva regla de implementación**.

3 En la página **Nombre y hosts** del asistente, escriba un nombre para la nueva regla.

4 Seleccione la opción para aplicar la regla a todos los hosts en el inventario o solo a los hosts que coincidan con un patrón específico.

Puede seleccionar uno o varios patrones.

Por ejemplo, la regla se puede aplicar solo a los hosts de un dominio de vCenter Single Sign-On con un nombre de host específico o a los hosts que coincidan con un rango de IPv4 específico.

5 En la página **Configuración** del asistente, puede optar por incluir elementos en la regla.

Cada elemento habilitado agrega una nueva página al asistente.

Opción	Acción
Ubicación de host	Agregue los hosts que coinciden con los criterios de la regla a una ubicación específica.
Perfil de imagen	Asigne un perfil de imagen a los hosts que coinciden con los criterios de la regla.

Opción	Acción
Perfil de host	Asigne un perfil de host a los hosts que coinciden con los criterios de la regla.
Paquete de scripts	Asigne un paquete de scripts a los hosts que coinciden con los criterios de la regla.

6 (opcional) En la página **Seleccionar ubicación de host** del asistente, seleccione un centro de datos, una carpeta o un clúster como ubicación de host para los hosts que coinciden con la regla.

7 (opcional) En la página **Seleccionar perfil de imagen** del asistente, utilice el menú desplegable para seleccionar un almacén de software y elija un perfil de imagen de la lista.

   Si quiere omitir la verificación del nivel de aceptación para el perfil de imagen, marque la casilla **Omitir comprobación de firma de perfil de imagen**.

8 (opcional) En la página **Seleccionar perfil de host** del asistente, elija un perfil de host de la lista.

9 (opcional) En la página **Seleccionar paquete de scripts** del asistente, seleccione un paquete de scripts de la lista.

10 En la página **Listo para completar**, revise la información resumida de la nueva regla.

Resultados

Para ver la regla recién creada, consulte la lista de la pestaña **Reglas de implementación**.

Pasos siguientes

- Active una regla de vSphere Auto Deploy. Consulte Activar, desactivar y reordenar las reglas de implementación.
- Edite una regla de vSphere Auto Deploy. Consulte Editar un perfil de imagen.
- Clone una regla de vSphere Auto Deploy. Consulte Clonar una regla de implementación
- Consulte la ubicación del host, el perfil de imagen, el perfil de host y los paquetes de scripts agregados. Consulte Ver asociaciones de hosts.
- Corrija los hosts que no cumplan con las reglas. Consulte Corregir un host no compatible.
- Cambie la asociación de perfil de imagen de un host. Consulte Editar la asociación de perfil de imagen de un host.

Clonar una regla de implementación

Puede usar una regla de vSphere Auto Deploy como plantilla y modificar solo partes de la regla en lugar de crear una nueva.

Puede clonar una regla de vSphere Auto Deploy por medio del asistente Clonar regla de implementación.

Requisitos previos

- Prepare el sistema e instale el servidor Auto Deploy. Para obtener más información, consulte Preparar el sistema para vSphere Auto Deploy.
- Cree una regla de vSphere Auto Deploy. Consulte Crear una regla de implementación.
- Si desea incluir un perfil de imagen en la regla, compruebe que se haya agregado el almacén de software necesario al inventario. Consulte Agregar un almacén de software o Importar un almacén de software.

Procedimiento

Procedimiento

1 Desplácese hasta **Inicio > Auto Deploy**.

De forma predeterminada, solo la función de administrador tiene privilegios para usar el servicio vSphere Auto Deploy.

2 En la pestaña **Reglas de implementación**, seleccione una regla de la lista.

3 Haga clic en **Clonar**.

Aparece el asistente **Clonar regla de implementación**.

4 En la página **Nombre y hosts** del asistente, escriba un nombre para la nueva regla.

5 Seleccione la opción para aplicar la regla a todos los hosts en el inventario o solo a los hosts que coincidan con un patrón específico.

Puede seleccionar uno o varios patrones.

Por ejemplo, la regla se puede aplicar solo a los hosts de un dominio de vCenter Single Sign-On con un nombre de host específico o a los hosts que coincidan con un rango de IPv4 específico.

6 En la página **Configuración** del asistente, puede optar por incluir elementos en la regla.

Cada elemento habilitado agrega una nueva página al asistente.

Opción	Acción
Ubicación de host	Agregue los hosts que coinciden con los criterios de la regla a una ubicación específica.
Perfil de imagen	Asigne un perfil de imagen a los hosts que coinciden con los criterios de la regla.
Perfil de host	Asigne un perfil de host a los hosts que coinciden con los criterios de la regla.
Paquete de scripts	Asigne un paquete de scripts a los hosts que coinciden con los criterios de la regla.

7 En la página **Seleccionar ubicación de host** del asistente, seleccione una ubicación para los hosts que coinciden con la regla.

Opción	Acción
Si desea mantener la ubicación del host usada en la regla clonada	Marque la casilla **Misma ubicación de host**.
Si desea seleccionar una nueva ubicación para los hosts seleccionados	1 Marque la casilla **Explorar ubicación de host**. 2 Seleccione un centro de datos, una carpeta o un clúster como ubicación de host. 3 Haga clic en **Siguiente**.

8 En la página **Seleccionar perfil de imagen** del asistente, seleccione un perfil de imagen.

Opción	Acción
Si no desea cambiar el perfil de imagen	Marque la casilla **Mismo perfil de imagen**.
Si desea asignar un nuevo perfil de imagen a los hosts seleccionados	1 Marque la casilla **Explorar perfil de imagen**. 2 Seleccione un almacén de software en el menú desplegable. 3 Seleccione un perfil de imagen de la lista. 4 (Opcional) Si desea omitir la verificación de nivel de aceptación para el perfil de imagen, active la casilla **Omitir comprobación de firma de perfil de imagen**.

9 En la página **Seleccionar perfil de host** del asistente, elija un perfil de host.

Opción	Acción
Si quiere mantener el perfil de host usado en la regla clonada	Marque la casilla **Mismo perfil de host**.
Si desea asignar un perfil de host nuevo a los hosts seleccionados	1 Marque la casilla **Explorar perfil de host**. 2 Seleccione un perfil de host en la lista y haga clic en **Siguiente**.

10 En la página **Seleccionar paquete de scripts** del asistente, seleccione un paquete de scripts de la lista.

11 En la página **Listo para completar**, revise la información resumida de la nueva regla.

Pasos siguientes

- Active una regla de vSphere Auto Deploy. Consulte Activar, desactivar y reordenar las reglas de implementación.
- Edite una regla de vSphere Auto Deploy. Consulte Editar un perfil de imagen.

Editar una regla de Auto Deploy

Puede editar el nombre de una regla de Auto Deploy inactiva, sus hosts coincidentes, la ubicación del host, el perfil de imagen y el perfil de host.

Requisitos previos

- Prepare el sistema e instale el servidor Auto Deploy. Para obtener más información, consulte Preparar el sistema para vSphere Auto Deploy.
- Cree una regla de vSphere Auto Deploy. Consulte Crear una regla de implementación.

Procedimiento

1 Desplácese hasta **Inicio > Auto Deploy**.

De forma predeterminada, solo la función de administrador tiene privilegios para usar el servicio vSphere Auto Deploy.

2 En la pestaña **Reglas de implementación**, seleccione la regla entre la lista de reglas del inventario y haga clic en **Editar**.

Se mostrará el cuadro de diálogo Editar regla de implementación.

3 (opcional) En la página **Nombre y hosts** del asistente, escriba un nuevo nombre para la regla.

4 Seleccione la opción para aplicar la regla a todos los hosts en el inventario o solo a los hosts que coincidan con un patrón específico.

Puede seleccionar uno o varios patrones.

Por ejemplo, la regla se puede aplicar solo a los hosts de un dominio de vCenter Single Sign-On con un nombre de host específico o a los hosts que coincidan con un rango de IPv4 específico.

5 En la página **Configuración** del asistente, puede optar por incluir elementos en la regla.

Cada elemento habilitado agrega una nueva página al asistente.

Opción	Acción
Ubicación de host	Agregue los hosts que coinciden con los criterios de la regla a una ubicación específica.
Perfil de imagen	Asigne un perfil de imagen a los hosts que coinciden con los criterios de la regla.
Perfil de host	Asigne un perfil de host a los hosts que coinciden con los criterios de la regla.
Paquete de scripts	Asigne un paquete de scripts a los hosts que coinciden con los criterios de la regla.

6 En la página **Seleccionar ubicación de host** del asistente, seleccione una ubicación para los hosts que coinciden con la regla.

Opción	Acción
Si desea mantener la ubicación del host usada en la regla clonada	Marque la casilla **Misma ubicación de host**.
Si desea seleccionar una nueva ubicación para los hosts seleccionados	1 Marque la casilla **Explorar ubicación de host**. 2 Seleccione un centro de datos, una carpeta o un clúster como ubicación de host. 3 Haga clic en **Siguiente**.

7 En la página **Seleccionar perfil de imagen** del asistente, seleccione un perfil de imagen.

Opción	Acción
Si no desea cambiar el perfil de imagen	Marque la casilla **Mismo perfil de imagen**.
Si desea asignar un nuevo perfil de imagen a los hosts seleccionados	1 Marque la casilla **Explorar perfil de imagen**. 2 Seleccione un almacén de software en el menú desplegable. 3 Seleccione un perfil de imagen de la lista. 4 (Opcional) Si desea omitir la verificación de nivel de aceptación para el perfil de imagen, active la casilla **Omitir comprobación de firma de perfil de imagen**.

8 En la página **Seleccionar perfil de host** del asistente, elija un perfil de host.

Opción	Acción
Si quiere mantener el perfil de host usado en la regla clonada	Marque la casilla **Mismo perfil de host**.
Si desea asignar un perfil de host nuevo a los hosts seleccionados	1 Marque la casilla **Explorar perfil de host**. 2 Seleccione un perfil de host en la lista y haga clic en **Siguiente**.

9 En la página **Seleccionar paquete de scripts** del asistente, seleccione un paquete de scripts de la lista.

10 En la página **Listo para completar**, revise la información resumida de la nueva regla.

Pasos siguientes

- Active una regla de vSphere Auto Deploy. Consulte Activar, desactivar y reordenar las reglas de implementación.
- Clone una regla de vSphere Auto Deploy. Consulte Clonar una regla de implementación

Activar, desactivar y reordenar las reglas de implementación

Después de crear una regla de vSphere Auto Deploy, la regla queda en estado inactivo. Debe activar la regla para que se aplique.

La lista superior de la página **Activar y reordenar** del asistente muestra las reglas del conjunto de reglas activo. La lista inferior muestra las reglas inactivas.

Requisitos previos

Puede usar el asistente Activar y reordenar para activar y desactivar reglas y para cambiar su orden.

- Prepare el sistema e instale el servidor Auto Deploy. Para obtener más información, consulte Preparar el sistema para vSphere Auto Deploy.
- Cree una regla de vSphere Auto Deploy. Consulte Crear una regla de implementación.

Procedimiento

1 Desplácese hasta **Inicio > Auto Deploy**.

   De forma predeterminada, solo la función de administrador tiene privilegios para usar el servicio vSphere Auto Deploy.

2 En la pestaña **Reglas de implementación**, haga clic en **Activar/desactivar reglas**.

   Aparece el asistente Activar y reordenar.

3 (opcional) Si desea desactivar una regla activa, seleccione la regla de la lista de reglas activas y haga clic en el botón **Desactivar**.

4 En la lista de reglas inactivas, seleccione la regla que desea activar y haga clic en el botón **Activar**.

5 (opcional) Si quiere cambiar el orden de las reglas en la lista de reglas activas, seleccione la regla que subirá o bajará en la lista; a continuación, haga clic en **Subir** o **Bajar** encima de la lista de reglas activas.

   Las reglas se ordenan por prioridad. Por ejemplo, si se aplican dos o más reglas al mismo host, pero se definen para que aprovisionen el host con distintas ubicaciones de host, perfiles de imagen y perfiles de host, se aplicará la regla con la posición más alta de la lista al host.

6 (opcional) Si quiere probar una regla inactiva antes de la activación, haga clic en **Probar reglas antes de la activación**.

   a Seleccione un host de la lista y haga clic en **Comprobar cumplimiento** para ver el estado actual del host y los cambios que se esperan después de la activación de la regla.

      Si el host cumple con la regla, no es necesario corregir el host tras activar la regla.

   b (opcional) Si quiere corregir los hosts seleccionados después de la activación de la regla, habilite el botón de alternancia o marque la casilla **Corregir todas las asociaciones de hosts después de activar reglas** para corregir todos los hosts.

7 Revise la lista de reglas activas y haga clic en **Aceptar**.

Resultados

En la pestaña **Reglas de implementación**, la regla se muestra como activa en la columna Estado.

Pasos siguientes

- Consulte la ubicación del host, el perfil de imagen, el perfil de host y los paquetes de scripts agregados. Consulte Ver asociaciones de hosts.
- Corrija los hosts que no cumplan con las reglas. Consulte Corregir un host no compatible.

Ver asociaciones de hosts

Es posible que algunos hosts ESXi del inventario de vSphere Auto Deploy no cumplan con las reglas de implementación activas y se deba comprobar el cumplimiento.

Requisitos previos

- Prepare el sistema e instale el servidor Auto Deploy. Para obtener más información, consulte Preparar el sistema para vSphere Auto Deploy.
- Cree una regla de vSphere Auto Deploy. Consulte Crear una regla de implementación.
- Active una regla de vSphere Auto Deploy. Consulte Activar, desactivar y reordenar las reglas de implementación.

Procedimiento

1 Desplácese hasta **Inicio > Auto Deploy**.

De forma predeterminada, solo la función de administrador tiene privilegios para usar el servicio vSphere Auto Deploy.

2 Compruebe el cumplimiento de las asociaciones de hosts.

La ventana **Comprobar cumplimiento de asociaciones de hosts** muestra el estado del host y si este cumple con el conjunto de reglas activas. Puede ver la ubicación de host, el perfil de imagen, el perfil de host, el perfil de host, el paquete de scripts y las asociaciones que están asignados actualmente y que entrarán en efecto después de corregir el host.

Opción	Pasos
Si quiere comprobar el cumplimiento de las asociaciones de hosts de un solo host	1 En la pestaña **Hosts implementados**, seleccione un host ESXi. 2 Haga clic en **Comprobar cumplimiento de asociaciones de hosts**. 3 Compruebe si las asociaciones de hosts cumplen con el conjunto de reglas activas actual. 4 (opcional) Si quiere corregir el host, haga clic en **Corregir**. 5 Cierre la ventana **Comprobar cumplimiento de asociaciones de hosts**.
Si quiere comprobar el cumplimiento de las asociaciones de hosts de varios hosts	1 En la pestaña **Hosts implementados**, seleccione varios hosts ESXi. 2 Haga clic en **Comprobar cumplimiento de asociaciones de hosts**. 3 Confirme que quiere comprobar el cumplimiento de todos los hosts seleccionados. 4 Revise el estado de cumplimiento de los hosts en el panel izquierdo. 5 (Opcional) Seleccione un host para ver los detalles de estado de cumplimiento. 6 (Opcional) Seleccione un host y haga clic en **Corregir** . 7 (Opcional) Seleccione la casilla **Corregir todas las asociaciones de host después de activar las reglas** para corregir todos los hosts. 8 **Cierre la ventana Comprobar cumplimiento de asociaciones de hosts**.

Pasos siguientes

- Corrija los hosts que no cumplan con las reglas. Consulte Corregir un host no compatible.
- Edite la asociación de perfil de imagen de un host. Consulte Editar la asociación de perfil de imagen de un host.
- Edite una regla de vSphere Auto Deploy. Consulte Editar un perfil de imagen.

Editar la asociación de perfil de imagen de un host

Puede editar la asociación de perfil de imagen de un solo host si el host no está asociado a una regla de vSphere Auto Deploy.

Requisitos previos

Como alternativa, es posible que no desee cambiar la asociación del perfil de imagen de varios hosts mediante la edición de una regla.

- Prepare el sistema e instale el servidor Auto Deploy. Para obtener más información, consulte Preparar el sistema para vSphere Auto Deploy.
- Cree una regla de vSphere Auto Deploy. Consulte Crear una regla de implementación.
- Active una regla de vSphere Auto Deploy. Consulte Activar, desactivar y reordenar las reglas de implementación.

Procedimiento

1 Desplácese hasta **Inicio > Auto Deploy**.

   De forma predeterminada, solo la función de administrador tiene privilegios para usar el servicio vSphere Auto Deploy.

2 En la pestaña **Hosts implementados**, seleccione un host ESXi.

3 Haga clic en **Editar asociación de perfil de imagen**.

   Aparece el cuadro de diálogo Editar asociación de perfil de imagen.

4 Edite la asociación de perfil de imagen del host.

Opción	Acción
Si no desea cambiar el perfil de imagen	Marque la casilla **Mismo perfil de imagen**.
Si desea asignar un nuevo perfil de imagen a los hosts seleccionados	1 Marque la casilla **Explorar perfil de imagen**. 2 Seleccione un almacén de software en el menú desplegable. 3 Seleccione un perfil de imagen de la lista. 4 (Opcional) Si desea omitir la verificación de nivel de aceptación para el perfil de imagen, active la casilla **Omitir comprobación de firma de perfil de imagen**.

5 Haga clic en **Aceptar**.

Resultados

El nuevo perfil de imagen figura en la columna Perfil de imagen asociado después de actualizar la página.

Pasos siguientes

- Consulte la ubicación del host, el perfil de imagen, el perfil de host y los paquetes de scripts agregados. Consulte Ver asociaciones de hosts.
- Si el host está asociado a una regla y desea revertirlo al perfil de imagen definido en la regla, debe corregir el host. Consulte Corregir un host no compatible.

Corregir un host no compatible

Corrija las asociaciones de hosts ESXi cuando agregue una regla al conjunto de reglas activo de vSphere Auto Deploy o realice cambios en una o varias reglas.

Requisitos previos

Cuando se agrega una regla al conjunto de reglas activas de vSphere Auto Deploy o cuando se realizan cambios en una regla o más, los hosts no se actualizan automáticamente. Debe corregir las asociaciones de host para aplicar las nuevas reglas al host.

- Prepare el sistema e instale el servidor Auto Deploy. Para obtener más información, consulte Preparar el sistema para vSphere Auto Deploy.
- Cree una regla de vSphere Auto Deploy. Consulte Crear una regla de implementación.
- Active una regla de vSphere Auto Deploy. Consulte Activar, desactivar y reordenar las reglas de implementación.
- Si al corregir un host se produce un cambio en su ubicación, debe ponerse al host en modo de mantenimiento.

Procedimiento

1. Desplácese hasta **Inicio > Auto Deploy**.

   De forma predeterminada, solo la función de administrador tiene privilegios para usar el servicio vSphere Auto Deploy.

2. En la pestaña **Hosts implementados**, seleccione uno o varios hosts ESXi.
3. Haga clic en **Corregir asociaciones de hosts**.

   Si corrige un host que tiene una asociación de perfil de imagen editada, el host vuelve a la configuración definida en la regla con la que coincide.

   Puede supervisar el progreso del proceso de corrección en el panel Tareas recientes.

Pasos siguientes

- Consulte la ubicación del host, el perfil de imagen, el perfil de host y los paquetes de scripts agregados. Consulte Ver asociaciones de hosts.

- Cambie la asociación de perfil de imagen de un host. Consulte Editar la asociación de perfil de imagen de un host.

Agregar un host al inventario de vSphere Auto Deploy

Puede ver los hosts que no coinciden con ninguna de las reglas de vSphere Auto Deploy y agregar manualmente un host al inventario de vSphere Auto Deploy.

Para agregar un host al inventario actual de hosts implementados de vSphere Auto Deploy, puede crear una nueva regla o editar una regla existente para incluir un host no implementado con vSphere Auto Deploy y asociarlo con una ubicación de host, un perfil de imagen, un perfil de host y un paquete de scripts específicos. Como alternativa, puede agregar un host al inventario manualmente si le asigna una ubicación de host, un perfil de imagen, un perfil de host y un paquete de scripts.

Requisitos previos

- Prepare el sistema e instale el servidor Auto Deploy. Para obtener más información, consulte Preparar el sistema para vSphere Auto Deploy.
- Para asignar un perfil de imagen al host, agregue al inventario el almacén de software que necesita. Consulte Agregar un almacén de software o Importar un almacén de software.

Procedimiento

Procedimiento

1 Desplácese hasta **Inicio > Auto Deploy**.

De forma predeterminada, solo la función de administrador tiene privilegios para usar el servicio vSphere Auto Deploy.

2 En la pestaña **Hosts detectados**, seleccione uno o más hosts que desee aprovisionar con una ubicación de host, un perfil de imagen y un perfil de host.

3 Seleccione **Agregar al inventario**.

Si lo prefiere,, haga clic en **Quitar** para descartar los hosts seleccionados desde la pestaña **Hosts detectados**.

Aparece el asistente Agregar al inventario.

4 En la página **Seleccionar ubicación de host** del asistente, seleccione un centro de datos, una carpeta o un clúster como ubicación de host para los hosts que coinciden con la regla.

5 En la página **Seleccionar perfil de imagen** del asistente, utilice el menú desplegable para seleccionar un almacén de software y elija un perfil de imagen de la lista.

Si quiere omitir la verificación del nivel de aceptación para el perfil de imagen, marque la casilla **Omitir comprobación de firma de perfil de imagen**.

6 En la página **Seleccionar perfil de host** del asistente, elija un perfil de host de la lista.

7 En la página **Seleccionar perfil de host** del asistente, utilice la opción **Filtrar** para buscar en la lista de perfiles de host o seleccione la casilla **No incluir un perfil de host** para continuar sin agregar un perfil de host.

8 En la página **Seleccionar paquete de scripts** del asistente, seleccione un paquete de scripts de la lista.

9 En la página Listo para finalizar, revise las asociaciones de hosts seleccionadas.

Pasos siguientes

- Edite una regla de vSphere Auto Deploy. Consulte Editar un perfil de imagen.
- Clone una regla de vSphere Auto Deploy. Consulte Clonar una regla de implementación
- Consulte la ubicación del host, el perfil de imagen, el perfil de host y los paquetes de scripts agregados. Consulte Ver asociaciones de hosts.
- Corrija los hosts que no cumplan con las reglas. Consulte Corregir un host no compatible.

Agregar un host a un clúster que utiliza una sola imagen

Cree una regla en Auto Deploy que asigne un clúster que administre mediante una sola imagen como la ubicación de host para los hosts ESXi recién agregados.

Al crear una regla de Auto Deploy, en la cual la ubicación de destino del host es un clúster administrado por una imagen, puede realizar una transición de los hosts ESXi con estado al clúster. La regla agrega los hosts al clúster de destino basándose en mecanismos de identificación de host.

Esta regla de Auto Deploy no puede contener un perfil de imagen ni un perfil de host, ya que la especificación de imagen y la configuración de los hosts en el clúster de destino se crean automáticamente.

Requisitos previos

Para agregar hosts ESXi a un clúster que se administra mediante una imagen única, cree una regla en Auto Deploy que asigne dicho clúster como ubicación del host para los nuevos hosts añadidos. Cada host hereda la misma imagen, lo que permite la comprobación de compatibilidad del hardware, la corrección en todo el clúster y actualizaciones más sencillas.

- Prepare el sistema e instale el servidor Auto Deploy. Para obtener más información, consulte *Preparar el sistema para vSphere Auto Deploy* en la documentación *Instalar y configurar VMware ESXi*.
- Confirme que la versión de cada host ESXi sea 8.0 o posterior.
- Confirme que todos los hosts del clúster tienen un estado y tienen asociado un almacenamiento físico.
- Confirme que las soluciones que no están integradas con vSphere Lifecycle Manager no están habilitadas en el clúster.

Procedimiento

1 Desplácese hasta **Inicio > Auto Deploy**.

De forma predeterminada, solo la función de administrador tiene privilegios para usar el servicio vSphere Auto Deploy.

2 En la pestaña **Reglas de implementación**, haga clic en **Nueva regla de implementación**.

Aparece el asistente **Nueva regla de implementación**.

3 En la página **Nombre y hosts** del asistente, escriba un nombre para la nueva regla.

4 Seleccione la opción para aplicar la regla a todos los hosts en el inventario o solo a los hosts que coincidan con un patrón específico.

Puede seleccionar uno o varios patrones.

Por ejemplo, la regla se puede aplicar solo a los hosts de un dominio de vCenter Single Sign-On con un nombre de host específico o a los hosts que coincidan con un rango de IPv4 específico.

5 En la página **Configuración** del asistente, active la casilla **Ubicación del host** y haga clic en **Siguiente**.

De forma opcional, puede incluir un paquete de scripts en los hosts ESXi que coincidan con los criterios de la regla. Para ello, active la casilla **Paquete de scripts**.

Nota Se utilizan el perfil de imagen y el perfil de host asociados al clúster de destino.

6 En la página **Seleccionar ubicación de host** del asistente, seleccione un clúster que utilice una sola imagen.

7 En la página **Seleccionar paquete de scripts** del asistente, seleccione un paquete de scripts de la lista.

8 En la página **Listo para completar**, revise la información resumida de la nueva regla.

9 Haga clic en **Finalizar**.

Resultados

Para ver la regla recién creada, consulte la lista de la pestaña **Reglas de implementación**.

Pasos siguientes

- Active una regla de vSphere Auto Deploy. Consulte Activar, desactivar y reordenar las reglas de implementación.
- Para obtener más información sobre el almacenamiento en caché sin estado y las instalaciones con estado, consulte Usar vSphere Auto Deploy para almacenamiento en caché sin estado e instalaciones con estado.

Agregar un host a un clúster que administra la configuración de ESXi a nivel de clúster

Cree una regla en Auto Deploy que asigne hosts recién agregados a un clúster que administre la configuración de ESXi a nivel de clúster.

Al crear una regla de Auto Deploy, donde la ubicación de destino del host es un clúster que administra la configuración de ESXi en un nivel de clúster, se elimina la necesidad de utilizar perfiles de host o realizar configuraciones manuales, a la vez que se mantiene la flexibilidad para definir la configuración personalizada por host o anular la configuración de nivel de clúster para un grupo de hosts. Para obtener más información sobre cómo configurar los clústeres que se administran con una configuración a nivel de clúster y los VMware vSphere Configuration Profiles, consulte Usar vSphere Configuration Profiles para administrar la configuración de hosts en un nivel de clúster.

Nota Una vez que se configura un clúster que administra la configuración de ESXi en un nivel de clúster, no se puede revertir al uso de perfiles de host o imágenes únicas, y no se puede utilizar la opción de inicio rápido para esos clústeres. Sin embargo, sí se puede cambiar de un clúster que administre con una sola imagen a un clúster que administre con una configuración a nivel de clúster. Para ello, solo tiene que seleccionar la opción **Establecer configuración de hosts** en **Configurar > Estado deseado > Configuración del host**.

Requisitos previos

Para agregar hosts ESXi a un clúster que administra la configuración de ESXi en un nivel de clúster, se crea una regla en Auto Deploy que asigna ese clúster como la ubicación de host para los hosts recién agregados, los cuales heredan la misma configuración y no requieren una configuración manual.

- Prepare el sistema e instale el servidor Auto Deploy. Para obtener más información, consulte Instalar y configurar vSphere Auto Deploy.
- Confirme que la versión de cada host ESXi sea 8.0 o posterior.

Procedimiento

1. Desplácese hasta **Inicio > Auto Deploy**.

   De forma predeterminada, solo la función de administrador tiene privilegios para usar el servicio vSphere Auto Deploy.

2. En la pestaña **Reglas de implementación**, haga clic en **Nueva regla de implementación**.

   Aparece el asistente **Nueva regla de implementación**.

3. En la página **Nombre y hosts** del asistente, escriba un nombre para la nueva regla.

4. Seleccione la opción para aplicar la regla a todos los hosts en el inventario o solo a los hosts que coincidan con un patrón específico.

   Puede seleccionar uno o varios patrones.

Por ejemplo, la regla se puede aplicar solo a los hosts de un dominio de vCenter Single Sign-On con un nombre de host específico o a los hosts que coincidan con un rango de IPv4 específico.

5 En la página **Configuración** del asistente, active la casilla **Ubicación del host** y haga clic en **Siguiente**.

   Puede ignorar las casillas **Imagen**, **Configuración del host** y **Paquete de scripts**. La especificación y configuración de imágenes de los hosts en el clúster de destino, así como cualquier configuración posterior a la instalación, se crean automáticamente. Incluso si selecciona alguna de las casillas, la regla ignorará las selecciones.

6 En la página **Seleccionar ubicación de host** del asistente, seleccione un clúster que administre la configuración de ESXi en un nivel de clúster.

7 En la página **Listo para completar**, revise la información resumida de la nueva regla.

8 Haga clic en **Finalizar**.

Resultados

Para ver la regla recién creada, consulte la lista de la pestaña **Reglas de implementación**.

Pasos siguientes

- Active una regla de vSphere Auto Deploy. Consulte Activar, desactivar y reordenar las reglas de implementación.
- Para obtener más información sobre el almacenamiento en caché sin estado y las instalaciones con estado, consulte Usar vSphere Auto Deploy para almacenamiento en caché sin estado e instalaciones con estado.

Trabajar con paquetes de scripts

Puede agregar un script personalizado para aplicar una configuración adicional de hosts posterior a la implementación. El script se ejecuta después de aprovisionar un host ESXi con Auto Deploy. Por ejemplo, puede crear una regla de firewall personalizada de ESXi y otras configuraciones que no están disponibles con los perfiles de host.

A partir de vSphere 6.7 Update 1, puede agregar o quitar un script personalizado mediante vSphere Client. Un paquete de scripts puede incluir varios scripts y debe entregarse como un único archivo comprimido con la extensión `.tgz`. Una vez cargado en vCenter Server, puede incluir el paquete de scripts en una regla de Auto Deploy.

Requisitos previos

- Compruebe que puede ejecutar el script en ESXi Shell.

Procedimiento

1 Desplácese hasta **Inicio > Auto Deploy**.

De forma predeterminada, solo la función de administrador tiene privilegios para usar el servicio vSphere Auto Deploy.

2 Seleccione la pestaña **Paquetes de scripts**.

3 Haga clic en **Cargar**.

4 Desplácese hasta un archivo de paquete de scripts y seleccione **Cargar**.

El script figura en la lista **Paquetes de scripts**.

5 (opcional) Seleccione un paquete de scripts, haga clic en **Quitar** y confirme la selección.

El paquete de scripts se elimina de la lista.

Pasos siguientes

- Active una regla de vSphere Auto Deploy. Consulte Activar, desactivar y reordenar las reglas de implementación.
- Edite una regla de vSphere Auto Deploy. Consulte Editar un perfil de imagen.
- Clone una regla de vSphere Auto Deploy. Consulte Clonar una regla de implementación
- Consulte la ubicación del host, el perfil de imagen, el perfil de host y los paquetes de scripts agregados. Consulte Ver asociaciones de hosts.
- Corrija los hosts que no cumplan con las reglas. Consulte Corregir un host no compatible.
- Cambie la asociación de perfil de imagen de un host. Consulte Editar la asociación de perfil de imagen de un host.

Descargar registros de vSphere Auto Deploy

Puede usar la información de registro de vSphere Auto Deploy de vSphere Client para solucionar los problemas que experimente con vSphere Auto Deploy.

Requisitos previos

Use vSphere Client para iniciar sesión en la instancia de vCenter Server con la que se ha registrado vSphere Auto Deploy.

Procedimiento

1 Desplácese hasta**Inicio > Administración** y seleccione **Implementación > Configuración del sistema**.

2 Seleccione uno de los nodos para el que desea recuperar un paquete de soporte. El paquete de soporte contiene los registros de los servicios.

3 Haga clic en **Exportar paquete de soporte**.

4 Seleccione solo **Dispositivo virtual > Auto Deploy**.

5 Haga clic en el botón **Exportar paquete de soporte** para descargar los archivos de registro.

Iniciar, detener o reiniciar el servicio de vSphere Auto Deploy

Puede iniciar, detener o reiniciar el servicio de Auto Deploy en la interfaz de administración de vCenter Server.

Para iniciar, detener y reiniciar servicios en vCenter Server, utilice la interfaz de administración de vCenter Server.

Requisitos previos

Compruebe que dispone de acceso raíz a la interfaz de administración de vCenter Server.

Procedimiento

1 Inicie sesión en la interfaz de administración de vCenter Server, https://*dirección-IP-o-FQDN*:5480.

2 Haga clic en **Servicios**.

   El panel **Servicios** muestra una tabla con todos los servicios instalados. Puede ordenarlos por nombre, tipo de inicio, mantenimiento y estado.

3 Seleccione el servicio de **Auto Deploy** y, a continuación, seleccione la acción.

   Las acciones disponibles dependen de si el servicio de Auto Deploy ya está en ejecución o no.

   - Haga clic en **Reiniciar** para reiniciar el servicio.

     El reinicio del servicio requiere confirmar la acción y puede provocar que la funcionalidad de Auto Deploy deje de estar disponible temporalmente.

   - Haga clic en **Iniciar** para iniciar el servicio.
   - Haga clic en **Detener** para detener el servicio.

     Para detener el servicio se requiere confirmar la acción.

Aprovisionar hosts ESXi con vSphere Auto Deploy

Use vSphere Auto Deploy para aprovisionar y reaprovisionar cientos de hosts físicos con software ESXi.

Puede utilizar vSphere Auto Deploy para aprovisionar cientos de hosts físicos con software ESXi por primera vez (primer arranque), reiniciar hosts o reaprovisionar hosts con un perfil de imagen, un perfil de host, un script personalizado, una carpeta o una ubicación de clúster diferentes. También puede optar por aprovisionar los hosts con un perfil de imagen que no contenga archivos binarios de VMware Tools.

Aprovisionar sistemas ESXi con vSphere Auto Deploy

vSphere Auto Deploy pueden aprovisionar cientos de hosts físicos con software de ESXi, ya sea para el primer arranque, el reinicio o el reaprovisionamiento.

Se pueden aprovisionar los hosts que no ejecutaron previamente el software ESXi (primer arranque), así como reiniciar o reaprovisionar los hosts con un perfil de imagen, un perfil de host, un script personalizado o una ubicación de clúster o carpeta diferentes. El proceso de vSphere Auto Deploy varía según el estado del host y según los cambios que desea realizar el usuario.

Proceso de arranque de vSphere Auto Deploy

Al arrancar un host que desea aprovisionar o reaprovisionar con vSphere Auto Deploy, la infraestructura de vSphere Auto Deploy suministra el perfil de imagen y, opcionalmente, un perfil de host, una ubicación de vCenter Server y un paquete de scripts para ese host.

El proceso de arranque para los hosts que aún no se han aprovisionado con vSphere Auto Deploy (primer arranque) es distinto al de los hosts que sí se aprovisionaron con vSphere Auto Deploy y se agregaron a un sistema vCenter Server (arranque posterior).

Requisitos previos para primer arranque

Antes de un proceso de primer arranque, debe configurar el sistema. La configuración incluye las siguientes tareas, que se tratan más detalladamente en Instalar y configurar vSphere Auto Deploy.

- Configure un servidor DHCP que asigne una dirección IP a cada host durante el inicio y que apunte el host al servidor TFTP desde el que se va a descargar el cargador de arranque iPXE.
- Si los hosts que planea aprovisionar con vSphere Auto Deploy presentan un BIOS heredado, compruebe que el servidor vSphere Auto Deploy tenga una dirección IPv4. El arranque PXE con firmware de BIOS heredado solo se puede realizar mediante IPv4. El arranque PXE con firmware UEFI se puede realizar mediante IPv4 o IPv6.
- Identifique el perfil de imagen que se va a usar de una de las siguientes maneras.
  - Elija un perfil de imagen de ESXi de un almacén público.
  - (opcional) Cree un perfil de imagen personalizado mediante vSphere ESXi Image Builder y colóquelo en un almacén al que pueda acceder el servidor vSphere Auto Deploy. El perfil de imagen debe incluir un VIB de ESXi de base.
- (opcional) Si tiene un host de referencia en el entorno, exporte el perfil de host de este y defina una regla que aplique el perfil a uno o más hosts. Consulte Configurar un host de referencia de vSphere Auto Deploy.
- Especifique reglas para la implementación del host y agréguelas al conjunto de reglas activo.

Información general sobre el primer arranque

Cuando se arranca un host que aún no se ha aprovisionado con arranques de vSphere Auto Deploy (primer arranque), el host interactúa con varios componentes de vSphere Auto Deploy.

1. Cuando el administrador enciende un host, este inicia una secuencia de arranque PXE.

   El servidor DHCP asigna una dirección IP al host y le indica que debe ponerse en contacto con el servidor TFTP.

2. El host realiza esta acción y descarga el archivo iPXE (cargador de arranque ejecutable) y un archivo de configuración iPXE.

3 iPXE comienza a ejecutarse.

   El archivo de configuración le indica al host que realice una solicitud de arranque HTTP al servidor vSphere Auto Deploy. La solicitud HTTP incluye información de hardware y de red.

4 En respuesta, el servidor vSphere Auto Deploy realiza estas tareas:

   a Consulta al motor de reglas la información sobre el host.

   b Transmite los componentes especificados en la información de perfil de imagen, perfil de host opcional y ubicación de vCenter Server opcional.

5 El host arranca mediante el perfil de imagen.

   Si el servidor vSphere Auto Deploy proporcionó un perfil de host, este se aplica al host.

6 vSphere Auto Deploy agrega el host al sistema vCenter Server en el que está registrado vSphere Auto Deploy.

   a Si una regla especifica una carpeta o un clúster de destino en el sistema vCenter Server, el host se coloca en esa carpeta o ese clúster. La carpeta de destino debe estar dentro de un centro de datos.

   b Si no hay una regla que especifique la ubicación de un inventario de vCenter Server, vSphere Auto Deploy agrega el host al primer centro de datos que se muestra en la interfaz de usuario de vSphere Client.

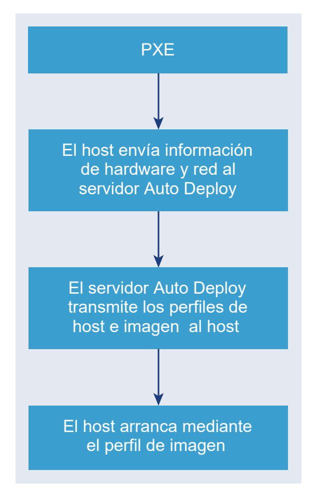
7 (opcional) Si el perfil de host requiere que el usuario especifique cierta información, como una dirección IP estática, el host se coloca en modo de mantenimiento cuando se agrega al sistema vCenter Server.

   Debe volver a aplicar el perfil de host y actualizar la personalización del host para que este salga del modo de mantenimiento. Al actualizar la personalización del host, debe responder las preguntas cuando se le pida.

8 Si el host forma parte de un clúster de DRS, las máquinas virtuales de otros hosts podrían migrarse al host después de que este se haya agregado correctamente al sistema vCenter Server.

Consulte Aprovisionar un host (primer arranque).

Figura 4-7. Instalación de vSphere Auto Deploy, primer arranque



Arranques posteriores sin actualizaciones

En el caso de los hosts aprovisionados con vSphere Auto Deploy y administrados por vCenter Server, los arranques posteriores pueden volverse completamente automáticos.

1 El administrador reinicia el host.

2 A medida que el host arranca, vSphere Auto Deploy lo aprovisiona con su perfil de imagen y su perfil de host.

3 Las máquinas virtuales se activan o se migran al host en base a la configuración del host.

- Host independiente. Las máquinas virtuales se encienden de acuerdo con las reglas de inicio automático definidas en el host.
- Host del clúster de DRS. Las máquinas virtuales que se migraron correctamente a otros hosts permanecen allí. Las máquinas virtuales para las que ningún host tenía recursos suficientes se registran en el host que se reinició.

Si vCenter Server no está disponible, el host se pone en contacto con el servidor vSphere Auto Deploy y se aprovisiona con un perfil de imagen. El host continúa poniéndose en contacto con el servidor vSphere Auto Deploy hasta que vSphere Auto Deploy vuelve a conectarse con vCenter Server.

vSphere Auto Deploy no puede configurar los conmutadores distribuidos de vSphere si vCenter Server no está disponible. Asimismo, las máquinas virtuales se asignan a hosts solo si forman parte de un clúster de vSphere HA. Una vez que el host vuelva a conectarse a vCenter Server y se aplique el perfil de host, podrá crear el conmutador. Debido a que el host se encuentra en modo de mantenimiento, no es posible iniciar las máquinas virtuales. Consulte Reaprovisionar hosts con operaciones de reinicio simples.

Los hosts que están configurados para pedir intervención del usuario se colocan en modo de mantenimiento. Consulte Actualizar la personalización de hosts en vSphere Client.

Arranques posteriores con actualizaciones

Es posible cambiar el perfil de imagen, el perfil de host, la ubicación de vCenter Server o el paquete de scripts de los hosts. El proceso involucra cambiar reglas, así como probar y reparar el cumplimiento de reglas del host.

1 El administrador utiliza el cmdlet `Copy-DeployRule` de PowerCLI para copiar y editar una o más reglas. A continuación, actualiza el conjunto de reglas. Consulte Introducción al proceso de vSphere Auto Deploy con PowerCLI para ver un ejemplo.

2 El administrador ejecuta el cmdlet `Test-DeployRulesetCompliance` para comprobar si cada host utiliza la información que especifica el conjunto de reglas actual.

3 El host devuelve un objeto de PowerCLI que encapsula la información de cumplimiento.

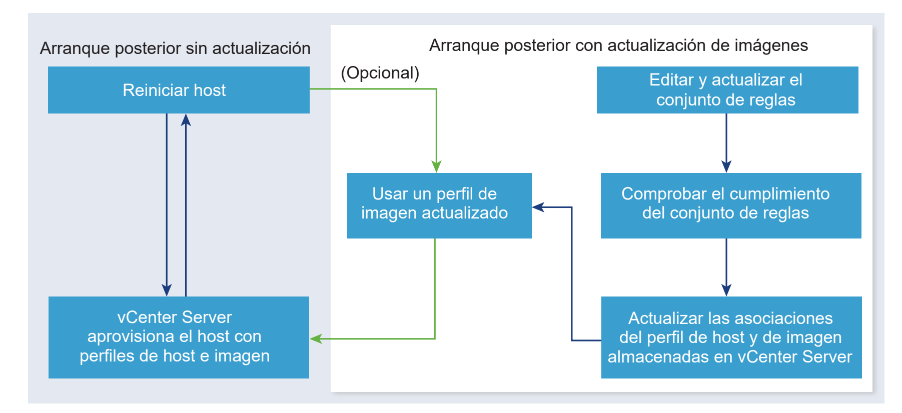
4 El administrador ejecuta el cmdlet `Repair-DeployRulesetCompliance` para actualizar el perfil de imagen, el perfil de host o la ubicación de vCenter Server que almacena el sistema vCenter Server para cada host.

5 Cuando el host se reinicia, utiliza el perfil de imagen, el perfil de host, la ubicación de vCenter Server o el paquete de scripts actualizados del host.

   Si el perfil de host está configurado para solicitar la intervención del usuario, el host se coloca en modo de mantenimiento. Siga los pasos descritos en Actualizar la personalización de hosts en vSphere Client.

Consulte Probar y reparar cumplimiento de reglas .

Figura 4-8. Instalación de vSphere Auto Deploy, arranques posteriores



Aprovisionar sistemas que tienen conmutadores distribuidos

Puede configurar el perfil de host de un host de referencia de vSphere Auto Deploy con un conmutador distribuido.

Cuando configura el conmutador distribuido, la directiva de parámetros de configuración de arranque se establece automáticamente para que coincida con los parámetros de red necesarios para la conectividad del host después de un reinicio.

Cuando vSphere Auto Deploy aprovisiona el host ESXi con el perfil de host, el host pasa por un proceso de dos pasos.

1 Crea un conmutador estándar virtual con las propiedades especificadas en el campo de parámetros de configuración de arranque.

2 Crea las NIC de VMkernel. Las NIC de VMkernel permiten que el host se conecte con vSphere Auto Deploy y el sistema vCenter Server.

Cuando el host se agrega a vCenter Server, vCenter Server elimina el conmutador estándar y vuelve a aplicar el conmutador distribuido al host.

Nota No modifique los parámetros de configuración de arranque del host para evitar problemas con el conmutador distribuido.

Aprovisionar un host (primer arranque)

Aprovisionar un host que nunca se aprovisionó con vSphere Auto Deploy (primer arranque) es una acción diferente a los procesos de arranque subsiguientes. Es necesario preparar el host y cumplir con todos los otros requisitos previos para poder aprovisionar el host. También puede definir un perfil de imagen personalizado con vSphere ESXi Image Builder mediante los cmdlets de vSphere Client o PowerCLI.

Requisitos previos

- Asegúrese de que el host cumpla con los requisitos de hardware para los hosts ESXi.

  Consulte Requisitos de hardware de ESXi.

- Prepare el sistema para vSphere Auto Deploy. Consulte Instalar y configurar vSphere Auto Deploy.

- Escriba reglas para asignar un perfil de imagen al host y para asignar, de forma opcional, un perfil de host y una ubicación de vCenter Server al host. Consulte Administrar vSphere Auto Deploy con cmdlets de PowerCLI o Administrar vSphere Auto Deploy con vSphere Client.

  Cuando se complete la instalación, el servicio vSphere Auto Deploy estará habilitado, la configuración de DHCP estará completada y las reglas para el host que desea aprovisionar se encontrarán en el conjunto de reglas activas.

Procedimiento

1 Encienda el host.

  El host se comunica con el servidor DHCP y descarga iPXE desde la ubicación que el servidor indica. A continuación, el servidor vSphere Auto Deploy aprovisiona al host con la imagen especificada por el motor de reglas. El servidor vSphere Auto Deploy también puede aplicar un perfil de host al host si existe uno especificado en el conjunto de reglas. Por último, vSphere Auto Deploy agrega el host al sistema vCenter Server especificado en el conjunto de reglas.

2 (opcional) Si vSphere Auto Deploy aplica un perfil de host que requiere alguna entrada del usuario, como una dirección IP, el host se coloca en el modo de mantenimiento. Vuelva a aplicar el perfil de host con vSphere Client y proporcione las entradas del usuario cuando se solicite.

Resultados

Después de un proceso de primer arranque, el host se ejecuta y administra a través de un sistema vCenter Server. vCenter Server almacena la información del perfil de imagen, el perfil de host y la ubicación del host.

Ahora puede reiniciar el host según sea necesario. Cada vez que reinicie, el host se reaprovisionará a través del sistema vCenter Server.

Pasos siguientes

Reaprovisione los hosts según sea necesario. Consulte Reaprovisionar hosts.

Si quiere cambiar el perfil de imagen, el perfil de host, el script personalizado o la ubicación del host, actualice las reglas y actívelas mediante vSphere Client o realice una operación de cumplimiento de prueba y reparación en una sesión de PowerCLI. Consulte Reglas y conjuntos de reglas o Probar y reparar cumplimiento de reglas .

Reaprovisionar hosts

Utilice vSphere Auto Deploy para reaprovisionar hosts ESXi con un perfil de imagen o un perfil de host diferente.

vSphere Auto Deploy admite varias opciones de reaprovisionamiento. Puede realizar un reinicio o un reaprovisionamiento sencillos con otro perfil de imagen o de host.

Para un primer arranque con vSphere Auto Deploy, debe configurar el entorno y agregar reglas al conjunto de reglas. Consulte Instalar y configurar vSphere Auto Deploy.

Están disponibles las siguientes operaciones de reaprovisionamiento.

- Reinicio simple.
- Reinicio de hosts sobre los que el usuario respondió preguntas durante la operación de arranque.
- Reaprovisionamiento con un perfil de imagen diferente.
- Reaprovisionamiento con un perfil de host diferente.

Reaprovisionar hosts con operaciones de reinicio simples

Puede reaprovisionar hosts ESXi con el perfil de imagen, el perfil de host, el script personalizado y la ubicación de vCenter Server asignada durante el primer arranque.

Requisitos previos

El reinicio simple de un host aprovisionado con vSphere Auto Deploy solo requiere que se sigan cumpliendo todos los requisitos previos. El proceso utiliza el perfil de imagen asignado previamente, el perfil de host, el script personalizado y la ubicación de vCenter Server.

- Compruebe que la configuración que realizó durante la primera operación de arranque esté vigente. Consulte Aprovisionar un host (primer arranque).
- Compruebe que todos los elementos asociados se encuentren disponibles. Un elemento puede ser un perfil de imagen, un perfil de host, un script personalizado o una ubicación de inventario de vCenter Server.
- Compruebe que el host contenga la información de identificación (etiqueta de activo, dirección IP) que tenía en las operaciones de arranque anteriores.

Procedimiento

1 Coloque el host en modo de mantenimiento.

Tipo de host	Acción
El host es parte de un clúster de DRS	VMware DRS migra las máquinas virtuales a los hosts adecuados cuando coloca el host en modo de mantenimiento.
El host no es parte de un clúster de DRS	Debe migrar todas las máquinas virtuales a distintos hosts y poner todos los hosts en modo de mantenimiento.

2 Reinicie el host.

Resultados

El host se apaga. Al reiniciarse, el host utiliza el perfil de imagen que proporciona el servidor vSphere Auto Deploy. El servidor vSphere Auto Deploy también aplica el perfil de host almacenado en el sistema vCenter Server.

Usar PowerCLI para reaprovisionar un host

Puede utilizar vSphere Auto Deploy para reaprovisionar un host con un nuevo perfil de imagen en una sesión de PowerCLI.

Existen varias opciones para reaprovisionar hosts.

- Si los VIB que desea usar son compatibles con la actualización directa, puede usar un comando `esxcli software vib update`. En ese caso, también debe actualizar el conjunto de reglas que se va a usar en un perfil de imagen que incluya los nuevos VIB.
- Durante las pruebas, puede aplicar un perfil de imagen a un host individual con el cmdlet `Apply-EsxImageProfile` y reiniciar el host para que el cambio sea efectivo. El cmdlet `Apply-EsxImageProfile` actualiza la asociación entre el host y el perfil de imagen, pero no instala ningún VIB en el host.
- En todos los demás casos, utilice este procedimiento.

Requisitos previos

- Compruebe que el perfil de imagen que desea utilizar para reaprovisionar el host se encuentre disponible. Utilice vSphere ESXi Image Builder en una sesión de PowerCLI. Consulte Personalizar instalaciones con vSphere ESXi Image Builder.
- Compruebe que la configuración que realizó durante la primera operación de arranque esté vigente.

Procedimiento

1 En la indicación de PowerShell, ejecute el cmdlet `Connect-VIServer` PowerCLI para conectarse al sistema vCenter Server con el que se registró vSphere Auto Deploy.

```
Connect-VIServer ipv4_or_ipv6_address
```

Es posible que el cmdlet devuelva una advertencia de certificado de servidor. En un entorno de producción, asegúrese de que no se emita ninguna advertencia de certificado de servidor. En un entorno de desarrollo, puede omitir la advertencia.

2 Determine la ubicación de un almacén de software público que contenga el perfil de imagen que desea utilizar o defina un perfil de imagen personalizado con vSphere ESXi Image Builder.

3 Ejecute `Add-EsxSoftwareDepot` para agregar el almacén de software que contiene el perfil de imagen a la sesión de PowerCLI.

Tipo de almacén	Cmdlet
Almacén remoto	Ejecute **`Add-EsxSoftwareDepot`** ***`url_del_almacén`***.
Archivo ZIP	a Descargue el archivo ZIP en una ruta de acceso de archivos local o cree un punto de montaje local en el equipo de PowerCLI. b Ejecute **`Add-EsxSoftwareDepot C:\file_path\my_offline_depot.zip`**.

4 Ejecute `Get-EsxImageProfile` para ver una lista de perfiles de imagen y determine qué perfil desea utilizar.

5 Ejecute `Copy-DeployRule` y especifique el parámetro `ReplaceItem` para cambiar la regla que asigna un perfil de imagen a hosts.

El siguiente cmdlet reemplaza el perfil de imagen actual que la regla asigna al host con el perfil *my_new_imageprofile*. Cuando el cmdlet finaliza, `myrule` asigna el nuevo perfil de imagen a los hosts. Se cambia el nombre de la antigua versión de `myrule` y se la oculta.

```
Copy-DeployRule myrule -ReplaceItem my_new_imageprofile
```

6 Pruebe el cumplimiento de reglas para cada host en el que desee implementar la imagen.

   a Compruebe que pueda acceder al host para el cual desea probar el cumplimiento del conjunto de reglas.

   ```
   Get-VMHost -Name ESXi_hostname
   ```

   b Ejecute el cmdlet que prueba el cumplimiento del conjunto de reglas para el host y vincule el valor devuelto a una variable para usarlo en otro momento.

   ```
   $tr = Test-DeployRuleSetCompliance ESXi_hostname
   ```

   c Examine las diferencias entre el contenido del conjunto de reglas y la configuración del host.

   ```
   $tr.itemlist
   ```

   El sistema devolverá una tabla de elementos actuales y esperados si el host en el que se desea probar el cumplimiento de un nuevo conjunto de reglas cumple con el conjunto de reglas activo.

   ```

   CurrentItem                              ExpectedItem
   -----------                              ------------
   my_old_imageprofile                            my_new_imageprofile
   ```

   d Corrija el host para que use el conjunto de reglas modificado la próxima vez que arranque.

   ```
   Repair-DeployRuleSetCompliance $tr
   ```

7 Reinicie el host para aprovisionarlo con el nuevo perfil de imagen.

Reaprovisionar un host con un nuevo perfil de imagen mediante vSphere Client

Puede usar vSphere Auto Deploy para reaprovisionar un host con un nuevo perfil de imagen con vSphere Client cambiando la regla a la que corresponde el host y activándola.

Requisitos previos

- Compruebe que el perfil de imagen que desea utilizar para reaprovisionar el host se encuentre disponible. Consulte Crear un perfil de imagen.
- Compruebe que la configuración que realizó durante la primera operación de arranque esté vigente.

Procedimiento

1 Desplácese hasta **Inicio > Auto Deploy**.

   De forma predeterminada, solo la función de administrador tiene privilegios para usar el servicio vSphere Auto Deploy.

2 En la pestaña **Reglas de implementación**, seleccione la regla entre la lista de reglas del inventario y haga clic en **Editar**.

Se mostrará el cuadro de diálogo Editar regla de implementación.

3 (opcional) En la página **Nombre y hosts** del asistente, escriba un nombre para la nueva regla.

4 (opcional) Seleccione la opción para aplicar la regla a todos los hosts en el inventario o solo a los hosts que coincidan con un patrón específico.

Puede seleccionar uno o varios patrones.

Por ejemplo, la regla se puede aplicar solo a los hosts de un dominio de vCenter Single Sign-On con un nombre de host específico o a los hosts que coincidan con un rango de IPv4 específico.

5 En la página **Configuración** del asistente, puede optar por incluir elementos en la regla.

Cada elemento habilitado agrega una nueva página al asistente.

Opción	Acción
Ubicación de host	Agregue los hosts que coinciden con los criterios de la regla a una ubicación específica.
Perfil de imagen	Asigne un perfil de imagen a los hosts que coinciden con los criterios de la regla.
Perfil de host	Asigne un perfil de host a los hosts que coinciden con los criterios de la regla.
Paquete de scripts	Asigne un paquete de scripts a los hosts que coinciden con los criterios de la regla.

6 Haga clic en **Siguiente** para omitir la selección de ubicación de host.

7 En la página **Seleccionar perfil de imagen** del asistente, asigne un perfil de imagen a los hosts que coincidan con los criterios de la regla.

Opción	Acción
Si no desea cambiar el perfil de imagen	Marque la casilla **Mismo perfil de imagen**.
Si desea asignar un nuevo perfil de imagen a los hosts seleccionados	1 Marque la casilla **Explorar perfil de imagen**. 2 Seleccione un almacén de software en el menú desplegable. 3 Seleccione un perfil de imagen de la lista. 4 (Opcional) Si desea omitir la verificación de nivel de aceptación para el perfil de imagen, active la casilla **Omitir comprobación de firma de perfil de imagen**.

8 Haga clic en **Siguiente** para omitir la selección de perfil de host.

9 En la página **Listo para completar**, revise la información resumida del nuevo perfil de imagen y haga clic en **Finalizar**.

10 Haga clic en **Activar/desactivar reglas**.

11 En la lista de reglas inactivas, seleccione la regla que desea activar y haga clic en el botón **Activar**.

12 (opcional) Si quiere cambiar el orden de las reglas en la lista de reglas activas, seleccione la regla que subirá o bajará en la lista; a continuación, haga clic en **Subir** o **Bajar** encima de la lista de reglas activas.

    Las reglas se ordenan por prioridad. Por ejemplo, si se aplican dos o más reglas al mismo host, pero se definen para que aprovisionen el host con distintas ubicaciones de host, perfiles de imagen y perfiles de host, se aplicará la regla con la posición más alta de la lista al host.

13 (opcional) Si quiere probar una regla inactiva antes de la activación, haga clic en **Probar reglas antes de la activación**.

    a Seleccione un host de la lista y haga clic en **Comprobar cumplimiento** para ver el estado actual del host y los cambios que se esperan después de la activación de la regla.

      Si el host cumple con la regla, no es necesario corregir el host tras activar la regla.

    b (opcional) Si quiere corregir los hosts seleccionados después de la activación de la regla, habilite el botón de alternancia o marque la casilla **Corregir todas las asociaciones de hosts después de activar reglas** para corregir todos los hosts.

14 Revise la lista de reglas activas y haga clic en **Aceptar**.

15 Reinicie el host para aprovisionarlo con el nuevo perfil de imagen.

Actualizar la personalización de hosts en vSphere Client

Si un host requería la intervención del usuario durante un arranque anterior, las respuestas estarán guardadas con vCenter Server. Si desea solicitar información nueva al usuario, debe corregir el host.

Requisitos previos

Conecte un perfil de host que solicite entrada de datos del usuario en el host.

Procedimiento

1 Migre todas las máquinas virtuales a distintos hosts y ponga el host en modo de mantenimiento.

Tipo de host	Acción
El host es parte de un clúster de DRS	VMware DRS migra las máquinas virtuales a los hosts adecuados cuando coloca el host en modo de mantenimiento.
El host no es parte de un clúster de DRS	Debe migrar todas las máquinas virtuales a distintos hosts y poner todos los hosts en modo de mantenimiento.

2 Desplácese hasta **Inicio > Auto Deploy**.

    De forma predeterminada, solo la función de administrador tiene privilegios para usar el servicio vSphere Auto Deploy.

3 En la pestaña **Hosts implementados**, seleccione un host ESXi.

4 Haga clic en **Corregir asociaciones de hosts**.

   Puede supervisar el progreso del proceso de corrección en el panel Tareas recientes.

5 Cuando se le solicite, proporcione la entrada de datos del usuario.

6 Dirija el host para salir del modo de mantenimiento.

Resultados

La personalización del host se guarda y se aplicará la próxima vez que arranque el host.

Aprovisionar hosts ESXi mediante un perfil de imagen sin VMware Tools

También puede optar por aprovisionar los hosts ESXi con un perfil de imagen que no contenga archivos binarios de VMware Tools.

Si el tiempo de arranque de la red es demasiado lento cuando se usa la imagen estándar, o si quiere ahorrar espacio en los hosts, puede usar un perfil de imagen que no incluya VMware Tools y puede colocar los binarios de VMware Tools en un almacenamiento compartido.

Requisitos previos

Cuando se aprovisionan hosts ESXi con vSphere Auto Deploy, puede optar por aprovisionarlos con un perfil de imagen que no contenga archivos binarios de VMware Tools. Este perfil de imagen es más pequeño, tiene una sobrecarga de memoria más baja y arranca con mayor rapidez en un entorno de arranque con PXE.

Descargue el perfil de imagen `xxxxx-no-tools` desde el sitio de descarga de VMware.

Procedimiento

1 Arranque un host ESXi que no se aprovisionó con vSphere Auto Deploy.

2 Copie el directorio `/productLocker` desde el host ESXi hasta un almacenamiento compartido.

   Para conectarse a un host ESXi mediante un cliente de SSH, consulte el artículo 1019852 de la Base de conocimientos.

3 Cambie la variable *UserVars.ProductLockerLocation* para que apunte a la nueva ubicación del directorio, `/productLocker`.

   a En vSphere Client, seleccione el host de referencia y haga clic en la pestaña **Configurar**.

   b En **Sistema**, haga clic en **Configuración avanzada del sistema**.

   c Haga clic en **Editar**.

   d Filtre la configuración para **`uservars`** y seleccione **UserVars.ProductLockerLocation**.

   e Haga clic en el valor actual y edite la ubicación de modo que apunte al almacenamiento compartido.

4 Cree un perfil de host desde el host de referencia.

5 Cree una regla de vSphere Auto Deploy que asigne el perfil de imagen `xxxxx-no-tools` y el perfil de host desde el host de referencia hasta todos los otros hosts.

6 Arranque sus host de destino con la regla para que elijan la ubicación del casillero del producto desde el host de referencia.

Usar vSphere Auto Deploy para almacenamiento en caché sin estado e instalaciones con estado

Con el almacenamiento en caché sin estado, puede almacenar en caché la imagen de un host ESXi. Con instalaciones con estado, puede instalar hosts a través de la red.

La función de almacenamiento en caché sin estado de vSphere Auto Deploy permite almacenar la imagen del host en la memoria caché. La función de instalaciones con estado de vSphere Auto Deploy permite instalar hosts por medio de la red. Después del primer arranque de red, estos hosts arrancan como cualquier otro host ESXi. La solución de almacenamiento en caché sin estado está destinada principalmente a las situaciones en las que varios hosts arrancan en simultáneo. La imagen almacenada en la memoria caché local ayuda a prevenir un cuello de botella que se produce si cientos de hosts se conectan simultáneamente al servidor vSphere Auto Deploy. Una vez finalizada la operación de arranque, los hosts se conectan a vSphere Auto Deploy para completar la configuración.

La característica de instalaciones con estado permite aprovisionar hosts con el perfil de imagen por medio de la red sin necesidad de configurar la infraestructura de arranque PXE.

Qué leer a continuación

- Introducción a almacenamiento en caché sin estado e instalaciones con estado

  Es posible usar el perfil de host de Configuración de la memoria caché del sistema para aprovisionar hosts con almacenamiento en caché sin estado e instalaciones con estado de vSphere Auto Deploy.

- Descripción general de las instalaciones con estado y el almacenamiento en caché sin estado

  Cuando desee utilizar vSphere Auto Deploy con almacenamiento en caché sin estado o con instalaciones con estado, deberá configurar un perfil de host, aplicar dicho perfil y establecer el orden de arranque.

Introducción a almacenamiento en caché sin estado e instalaciones con estado

Es posible usar el perfil de host de Configuración de la memoria caché del sistema para aprovisionar hosts con almacenamiento en caché sin estado e instalaciones con estado de vSphere Auto Deploy.

Ejemplos de almacenamiento en caché sin estado e instalaciones con estado

Hosts aprovisionados con vSphere Auto Deploy que almacenan en caché la imagen (almacenamiento en caché sin estado)

Configure y aplique un perfil de host para el almacenamiento en caché sin estado. Puede almacenar la imagen en la memoria caché de un disco local, un disco remoto o una unidad USB. Continúe aprovisionando este host con vSphere Auto Deploy. Si el servidor vSphere Auto Deploy no está disponible, por ejemplo, debido a que cientos de hosts intentan acceder a él de forma simultánea, el host arranca desde la memoria caché. Después de la operación de arranque, el host intenta comunicarse con el servidor vSphere Auto Deploy para completar la configuración.

Los hosts aprovisionados con vSphere Auto Deploy se convierten en hosts con estado

Configure y aplique un perfil de host para instalaciones con estado. Cuando aprovisiona un host con vSphere Auto Deploy, la imagen se instala en el disco local, un disco remoto o una unidad USB. Para arranques posteriores, hágalo desde el disco. El host ya no usa vSphere Auto Deploy.

Preparar

Para usar correctamente el almacenamiento en caché sin estado o instalaciones con estado, debe decidir cómo configurar el sistema y establecer el orden de arranque.

Tabla 4-19. Preparar almacenamiento en caché sin estado o instalaciones con estado

Requisito o decisión	Descripción
Decidir sobre la sobrescritura de la partición de VMFS	Cuando instale ESXi mediante el instalador interactivo, se le consulta si desea sobrescribir un almacén de datos existente de VMFS. El perfil de host de Configuración de la memoria caché del sistema proporciona una opción para sobrescribir particiones existentes de VMFS. La opción no está disponible si configura el perfil de host para que use una unidad USB.
Decidir si se necesita un entorno de alta disponibilidad	Si usa vSphere Auto Deploy con almacenamiento en caché sin estado, puede configurar un entorno de vSphere Auto Deploy de alta disponibilidad para garantizar que las máquinas virtuales migren a hosts aprovisionados recientemente y que el entorno admita vNetwork Distributed Switch incluso si el sistema vCenter Server queda temporalmente no disponible.
Establecer el orden de arranque	El orden de arranque que especifica para los hosts depende de la característica que desea usar. ■ Para configurar vSphere Auto Deploy con almacenamiento en caché sin estado, configure el host para que primero intente arrancar desde la red y, luego, intente arrancar desde el disco. Si el servidor vSphere Auto Deploy no está disponible, el host arranca usando la memoria caché. ■ Para configurar vSphere Auto Deploy para instalaciones con estado en hosts que actualmente no tienen un disco de arranque, configure sus hosts para que primero intenten arrancar desde el disco y, luego, intenten hacerlo desde la red. **Nota** Si actualmente tiene una imagen de arranque en el disco, configure los hosts para un arranque PXE único y aprovisione el host con vSphere Auto Deploy para que use un perfil de host que especifique instalaciones con estado.

Almacenamiento en caché sin estado y pérdida de conectividad

Si los hosts ESXi que se ejecutan en las máquinas virtuales pierden conectividad con el servidor vSphere Auto Deploy, el sistema vCenter Server, o ambos, se aplicarán algunas limitaciones la próxima vez que reinicie el host.

- Si vCenter Server está disponible, pero el servidor vSphere Auto Deploy no lo está, los hosts no se conectan al sistema vCenter Server de forma automática. Puede conectar manualmente los hosts a vCenter Server o esperar hasta que el servidor vSphere Auto Deploy vuelva a estar disponible.
- Si tanto vCenter Server como vSphere Auto Deploy no están disponibles, puede conectarse a cada host ESXi mediante VMware Host Client y agregar máquinas virtuales a cada host.

- Si vCenter Server no está disponible, vSphere DRS no funciona. El servidor vSphere Auto Deploy no puede agregar hosts a vCenter Server. Puede conectarse a cada host ESXi mediante VMware Host Client y agregar máquinas virtuales a cada host.
- Si realiza cambios a la configuración mientras está perdida la conectividad, los cambios se pierden cuando se restaura la conexión del servidor vSphere Auto Deploy.

Descripción general de las instalaciones con estado y el almacenamiento en caché sin estado

Cuando desee utilizar vSphere Auto Deploy con almacenamiento en caché sin estado o con instalaciones con estado, deberá configurar un perfil de host, aplicar dicho perfil y establecer el orden de arranque.

Cuando se aplica un perfil de host que permite el almacenamiento en caché en un host, vSphere Auto Deploy particiona el disco especificado. Lo que ocurre después depende de la forma en que configure el perfil de host y establezca el orden de arranque en el host.

- Si se ha seleccionado **Habilitar almacenamiento en caché sin estado en el host** en el perfil de host de configuración de caché del sistema, vSphere Auto Deploy almacenará la imagen en caché cuando aplique el perfil de host. No se requiere reiniciar. Cuando reinicie más tarde, el host continuará utilizando la infraestructura de vSphere Auto Deploy para recuperar su imagen. Si el servidor vSphere Auto Deploy no está disponible, el host utiliza la imagen almacenada en caché.
- vSphere Auto Deploy instala la imagen si **Habilitar instalaciones con estado en el host** está seleccionado en el perfil de host de configuración de caché del sistema. Al reiniciar, el host inicialmente arranca usando vSphere Auto Deploy para completar la instalación. A continuación se genera automáticamente un reinicio, después del cual el host arranca desde el disco, al igual que un host aprovisionado con el instalador. vSphere Auto Deploy ya no realiza el aprovisionamiento del host.

Puede aplicar el perfil del host desde vSphere Client o escribir una regla de vSphere Auto Deploy en una sesión de PowerCLI que aplique el perfil del host.

Usar vSphere Client para configurar vSphere Auto Deploy para el almacenamiento en caché sin estado o las instalaciones con estado

Puede crear un perfil de host en un host de referencia y aplicar dicho perfil de host a hosts adicionales, o a una carpeta o clúster de vCenter Server. Aparece el siguiente flujo de trabajo.

1 Aprovisione un host con vSphere Auto Deploy y edite el perfil de host de configuración de caché de imagen del sistema del host.

2 Coloque uno más hosts de destino en el modo de mantenimiento, aplique el perfil de host a cada host e indique al host que salga del modo de mantenimiento.

3 Lo que ocurra después depende del perfil de host seleccionado.

   - Si el perfil de host habilitó el almacenamiento en caché sin estado, la imagen se almacenará en caché en el disco. No se requiere reiniciar.
   - Si el perfil de host habilitó las instalaciones con estado, se instalará la imagen. Cuando reinicie, el host utilizará la imagen instalada.

Usar PowerCLI para configurar vSphere Auto Deploy para el almacenamiento en caché sin estado o las instalaciones con estado

Puede crear un perfil de host para un host de referencia y escribir una regla de vSphere Auto Deploy que aplique dicho perfil de host a otros hosts de destino en una sesión de PowerCLI. Aparece el siguiente flujo de trabajo.

1 Aprovisione un host de referencia con vSphere Auto Deploy y cree un perfil de host para habilitar una forma de almacenamiento en caché.
2 Escriba una regla que aprovisione hosts adicionales con vSphere Auto Deploy y que aplique el perfil de host de referencia a esos hosts.
3 vSphere Auto Deploy aprovisiona cada host con el perfil de imagen o mediante el uso del paquete de scripts asociado con la regla. El efecto exacto de aplicar el perfil de host depende del perfil del host seleccionado.
   - En el caso de instalaciones con estado, vSphere Auto Deploy procederá de la siguiente manera:
     - Durante el primer arranque, vSphere Auto Deploy instala la imagen en el host.
     - Durante los arranques siguientes, el host arranca desde el disco. Los hosts no necesitan una conexión al servidor vSphere Auto Deploy.
   - En el caso del almacenamiento en caché sin estado, vSphere Auto Deploy procederá de la siguiente manera:
     - Durante el primer arranque, vSphere Auto Deploy aprovisiona el host y almacena la imagen en caché.
     - Durante los arranques siguientes, vSphere Auto Deploy aprovisiona el host. Si vSphere Auto Deploy no está disponible, el host arranca desde la imagen almacenada en caché. Sin embargo, la configuración solo puede completarse cuando el host puede llegar al servidor vSphere Auto Deploy.

Configurar un perfil de host para utilizar el almacenamiento en caché sin estado

Si el servidor de vSphere Auto Deploy no está disponible, el host utiliza una imagen almacenada en caché y, para usar el almacenamiento en caché sin estado, debe configurar un perfil de host.

Requisitos previos

Cuando un host está configurado para usar almacenamiento en caché sin estado, si el servidor de vSphere Auto Deploy no está disponible, el host utiliza una imagen almacenada en caché. Para utilizar el almacenamiento en caché sin estado, debe configurar un perfil de host. Puede aplicar ese perfil a otros hosts que desee configurar para el almacenamiento en caché sin estado.

- Decida qué disco desea utilizar para almacenamiento en caché y determine si el proceso de almacenamiento en caché sobrescribirá una partición de VMFS existente.

- En los entornos de producción, incluya el sistema vCenter Server y el servidor vSphere Auto Deploy en un entorno altamente disponible para protegerlos. Tener vCenter Server en un clúster de administración garantiza que VDS y la migración de máquinas virtuales estén disponibles. De ser posible, proteja también otros elementos de la infraestructura. Consulte Configurar la infraestructura de vSphere Auto Deploy de alta disponibilidad.
- Configure el entorno de vSphere Auto Deploy. Consulte Instalar y configurar vSphere Auto Deploy.
- Compruebe que haya un disco con al menos 4GB de espacio libre disponible. Si el disco aún no está particionado, este procedimiento se lleva a cabo cuando aplica el perfil de host.
- Configure el host para que primero intente realizar un arranque de red y, si se produce un error, un arranque desde un disco. Consulte la documentación del proveedor de hardware.
- Cree un perfil de host. Consulte la documentación sobre *perfiles de host*.

Procedimiento

1 Desplácese hasta **Inicio > Directivas y perfiles > Perfiles de host**.

2 Haga clic en el perfil de host que quiere configurar y seleccione la pestaña **Configurar**.

3 Haga clic en **Editar perfil de host**.

4 En la página Editar perfil de host del asistente, seleccione **Opciones de configuración avanzadas > Configuración de memoria caché de imagen del sistema > Configuración de memoria caché de imagen del sistema**.

5 En el menú desplegable **Configuración de perfil de memoria caché de imagen del sistema**, elija una opción de directiva.

Opción	Descripción
Habilitar almacenamiento en caché sin estado en el host	Almacena en caché la imagen en el disco.
Habilitar almacenamiento en caché sin estado en un disco USB del host	Almacena en caché la imagen en un disco USB asociado al host.

6 En función de la opción de directiva que seleccione, debe hacer lo siguiente:

a Si selecciona **Habilitar almacenamiento en caché sin estado en el host**:

1 Especifique la información sobre el disco que se va a utilizar.

Opción	Descripción
Argumentos para el primer disco	Al configurar un disco de instalación de imagen del sistema, tiene varias opciones para definir el dispositivo en el que desea que ESXi se instale y desde el que quiere que se arranque. Puede utilizar los siguientes argumentos para definir el disco para la instalación: ■ **`localesx`**: el primer disco detectado que contiene una instalación válida de ESXi ■ **`local`**: el primer disco local detectado por ESXi después del arranque ■ **`remoteesx`**: el primer disco remoto detectado que contiene una instalación válida de ESXi ■ **`sortedremoteesx`**: el primer disco remoto ordenado por el identificador de LUN más bajo detectado que contiene una instalación válida de ESXi ■ **`remote`**: el primer disco remoto detectado por ESXi después del arranque ■ **`sortedremote`**: el primer disco remoto ordenado según el identificador de LUN más bajo detectado por ESXi después del arranque ■ **`modelo de dispositivo`** ■ **`proveedor de dispositivo`** ■ **`nombre de controlador de dispositivo de vmkernel`** Puede obtener los valores de los argumentos del proveedor y el modelo de dispositivo ejecutando el comando `esxcli storage core device list` en una consola para el host ESXi, iniciando sesión como raíz. Para obtener el argumento del nombre del controlador del dispositivo vmkernel, ejecute el comando `esxcli storage core adapter list`. Después debe identificar el adaptador de almacenamiento al que está conectado el dispositivo de arranque. De forma predeterminada, el sistema intenta reemplazar una instalación de ESXi existente y, a continuación, intenta escribir en el disco local. Puede utilizar el campo **Argumentos para primer disco** para especificar una lista separada por comas de los discos que se van a utilizar, en orden de preferencia. Puede especificar más de un disco. Use **`localesx`** para el primer disco con ESX instalado, la información del proveedor y el modelo; o bien, especifique el nombre del controlador del dispositivo de VMkernel. Por ejemplo, para que el sistema busque primero un disco con el nombre de modelo ST3120814A, segundo cualquier disco que utilice el controlador mptsas y tercero el disco local, especifique **`ST3120814A,mptsas,local`** como el valor para el campo. La primera configuración de disco del perfil de host especifica el orden de búsqueda para determinar qué disco se va a usar para la memoria caché. El orden de búsqueda se especifica como una lista de valores delimitados por comas. El valor predeterminado **`localesx,local`** especifica que vSphere Auto Deploy primero debe buscar un disco de memoria caché local existente. El disco de memoria caché se identifica

Opción	Descripción
	como un disco con la imagen del software ESXi existente. Si vSphere Auto Deploy no puede encontrar un disco de memoria caché existente, busca un dispositivo de disco local disponible. Al buscar un disco disponible, vSphere Auto Deploy usa el primer disco vacío que no contenga una partición de VMFS existente. Puede utilizar el primer argumento de disco solo para especificar el orden de búsqueda. No puede especificar un disco explícitamente. Por ejemplo, no puede especificar un determinado LUN o una SAN.
Marcar para sobrescribir los volúmenes VMFS en el disco seleccionado	Si activa esta casilla, el sistema sobrescribe los volúmenes VMFS existentes cuando no haya suficiente espacio disponible para almacenar la imagen, el perfil de imagen y el perfil de host.
Marcar para ignorar los dispositivos SSD conectados al host	Si activa esta casilla, el sistema omite todos los dispositivos SSD existentes y no almacena los perfiles de imagen ni los perfiles de host en ellos.

1. En el menú desplegable **Configuración de disco del sistema**, seleccione **Elección explícita de la opción de directiva por parte del usuario**.

b Si selecciona **Habilitar almacenamiento en caché sin estado en un disco USB del host**:

1. En el menú desplegable **Configuración de disco del sistema**, seleccione **Disco del sistema especificado por el usuario en la personalización del host**.
2. En **Hosts y clústeres**, haga clic con el botón derecho en el host y seleccione **Perfiles de host > Editar personalizaciones de host**. Defina un disco con almacenamiento persistente en el campo **Valor** para la propiedad **Disco del sistema**.

7 Haga clic en **Guardar** para completar la configuración del perfil de host.

Pasos siguientes

Aplique el perfil de host a los hosts individuales mediante la función Host Profiles en vSphere Client. Consulte la documentación sobre *perfiles de host*. Como alternativa, puede crear una regla para asignar el perfil de host a los hosts con vSphere Client o PowerCLI. Consulte Escribir una regla y asignar un perfil de host a hosts.

- Cree una regla que aplique el perfil de host a todos los hosts que desea aprovisionar con la configuración especificada en el host de referencia. Para escribir una regla en una sesión de PowerCLI, consulte Escribir una regla y asignar un perfil de host a hosts.
- Si los hosts ya se aprovisionaron con vSphere Auto Deploy, ejecute la prueba y repare las operaciones de cumplimiento en una sesión de PowerCLI. Para eso, consulte Probar y reparar cumplimiento de reglas .
- Encienda los hosts no aprovisionados para aprovisionarlos con el nuevo perfil de host.

Configurar un perfil de host para habilitar instalaciones con estado

Si desea configurar un host ESXi aprovisionado con vSphere Auto Deploy para el arranque desde el disco, debe configurar un perfil de host.

Puede configurar el perfil de host en un único host. También puede crear un perfil de host en un host de referencia y aplicarlo a otros hosts.

Requisitos previos

- Decida qué disco desea usar para almacenar la imagen y determine si la nueva imagen sobrescribirá una partición actual de VMFS.
- Configure el entorno de vSphere Auto Deploy. Consulte Instalar y configurar vSphere Auto Deploy.
- Compruebe que haya un disco con al menos 4GB de espacio libre disponible. Si el disco aún no está particionado, este procedimiento se lleva a cabo cuando aplica el perfil de host.
- Configure el host para arrancar desde el disco. Consulte la documentación del proveedor de hardware.
- Cree un perfil de host. Consulte la documentación sobre *perfiles de host*.

Procedimiento

1 Desplácese hasta **Inicio > Directivas y perfiles > Perfiles de host**.

2 Haga clic en el perfil de host que quiere configurar y seleccione la pestaña **Configurar**.

3 Haga clic en **Editar perfil de host**.

4 En la página Editar perfil de host del asistente, seleccione **Opciones de configuración avanzadas > Configuración de memoria caché de imagen del sistema > Configuración de memoria caché de imagen del sistema**.

5 En el menú desplegable **Configuración de perfil de memoria caché de imagen del sistema**, elija una opción de directiva.

Opción	Descripción
Habilitar instalaciones con estado en el host	Almacena la imagen en la memoria caché, en un disco.
Habilitar instalaciones con estado en un disco USB en el host	Almacena en caché la imagen en un disco USB asociado al host.

6 En función de la opción de directiva que seleccione, debe hacer lo siguiente:

a Si selecciona **Habilitar instalaciones con estado en el host**:

1 Especifique la información sobre el disco que se va a utilizar.

Opción	Descripción
Argumentos para el primer disco	Al configurar un disco de instalación de imagen del sistema, tiene varias opciones para definir el dispositivo en el que desea que ESXi se instale y desde el que quiere que se arranque. Puede utilizar los siguientes argumentos para definir el disco para la instalación: ■ **`localesx`**: el primer disco detectado que contiene una instalación válida de ESXi ■ **`local`**: el primer disco local detectado por ESXi después del arranque ■ **`remoteesx`**: el primer disco remoto detectado que contiene una instalación válida de ESXi ■ **`sortedremoteesx`**: el primer disco remoto ordenado por el identificador de LUN más bajo detectado que contiene una instalación válida de ESXi ■ **`remote`**: el primer disco remoto detectado por ESXi después del arranque ■ **`sortedremote`**: el primer disco remoto ordenado según el identificador de LUN más bajo detectado por ESXi después del arranque ■ **`modelo de dispositivo`** ■ **`proveedor de dispositivo`** ■ **`nombre de controlador de dispositivo de vmkernel`** Puede obtener los valores de los argumentos del proveedor y el modelo de dispositivo ejecutando el comando `esxcli storage core device list` en una consola para el host ESXi, iniciando sesión como raíz. Para obtener el argumento del nombre del controlador del dispositivo vmkernel, ejecute el comando `esxcli storage core adapter list`. Después debe identificar el adaptador de almacenamiento al que está conectado el dispositivo de arranque. De forma predeterminada, el sistema intenta reemplazar una instalación de ESXi existente y, a continuación, intenta escribir en el disco local. Puede utilizar el campo **Argumentos para primer disco** para especificar una lista separada por comas de los discos que se van a utilizar, en orden de preferencia. Puede especificar más de un disco. Use **`localesx`** para el primer disco con ESX instalado, la información del proveedor y el modelo; o bien, especifique el nombre del controlador del dispositivo de VMkernel. Por ejemplo, para que el sistema busque primero un disco con el nombre de modelo ST3120814A, segundo cualquier disco que utilice el controlador mptsas y tercero el disco local, especifique **`ST3120814A,mptsas,local`** como el valor para el campo. La primera configuración de disco del perfil de host especifica el orden de búsqueda para determinar qué disco se va a usar para la memoria caché. El orden de búsqueda se especifica como una lista de valores delimitados por comas. El valor predeterminado **`localesx,local`** especifica que vSphere Auto Deploy primero debe buscar un disco de memoria caché local existente. El disco de memoria caché se identifica

Opción	Descripción
	como un disco con la imagen del software ESXi existente. Si vSphere Auto Deploy no puede encontrar un disco de memoria caché existente, busca un dispositivo de disco local disponible. Al buscar un disco disponible, vSphere Auto Deploy usa el primer disco vacío que no contenga una partición de VMFS existente. Puede utilizar el primer argumento de disco solo para especificar el orden de búsqueda. No puede especificar un disco explícitamente. Por ejemplo, no puede especificar un determinado LUN o una SAN.
Marcar para sobrescribir los volúmenes VMFS en el disco seleccionado	Si activa esta casilla, el sistema sobrescribe los volúmenes VMFS existentes cuando no haya suficiente espacio disponible para almacenar la imagen, el perfil de imagen y el perfil de host.
Marcar para ignorar los dispositivos SSD conectados al host	Si activa esta casilla, el sistema omite todos los dispositivos SSD existentes y no almacena los perfiles de imagen ni los perfiles de host en ellos.

1. En el menú desplegable **Configuración de disco del sistema**, seleccione **Elección explícita de la opción de directiva por parte del usuario**.

b Si selecciona **Habilitar instalaciones con estado en un disco USB en el host**:

1. En el menú desplegable **Configuración de disco del sistema**, seleccione **Disco del sistema especificado por el usuario en la personalización del host**.
2. En **Hosts y clústeres**, haga clic con el botón derecho en el host y seleccione **Perfiles de host > Editar personalizaciones de host**. Defina un disco con almacenamiento persistente en el campo **Valor** para la propiedad **Disco del sistema**.

7 Haga clic en **Guardar** para completar la configuración del perfil de host.

Pasos siguientes

Aplique el perfil de host a los hosts individuales mediante la función Host Profiles en vSphere Client. Consulte la documentación sobre *perfiles de host*. Como alternativa, puede crear una regla para asignar el perfil de host a los hosts con vSphere Client o PowerCLI. Consulte Escribir una regla y asignar un perfil de host a hosts.

- Cree una regla que aplique el perfil de host a todos los hosts que desea aprovisionar con la configuración especificada en el host de referencia. Para escribir una regla en una sesión de PowerCLI, consulte Escribir una regla y asignar un perfil de host a hosts.
- Si los hosts ya se aprovisionaron con vSphere Auto Deploy, ejecute la prueba y repare las operaciones de cumplimiento en una sesión de PowerCLI. Para eso, consulte Probar y reparar cumplimiento de reglas .
- Encienda los hosts no aprovisionados para aprovisionarlos con el nuevo perfil de host.

Configurar un host de referencia de vSphere Auto Deploy

En un entorno donde no se almacena ningún estado en el host ESXi, un host de referencia ayuda a configurar varios hosts con la misma configuración.

Puede configurar el host de referencia con generación de registros, volcado de memoria y otra configuración que desea, guardar el perfil de host y escribir una regla que aplique el perfil de host a otros hosts según sea necesario. Puede ajustar la configuración de almacenamiento, conexión de redes y seguridad en el host de referencia y configurar servicios, como syslog y NTP.

Información sobre la configuración del host de referencia

Un host de referencia bien diseñado se conecta con todos los servicios, como syslog, NTP, etc. La configuración del host de referencia también podría incluir seguridad, almacenamiento, conexión de redes y ESXi Dump Collector. Puede aplicar la configuración de dicho host a otros hosts a través de los perfiles de host.

La configuración exacta de su host de referencia depende de su entorno, pero podría considerar la siguiente personalización.

Configuración de servidor NTP

Al recopilar información de generación de registros en entornos grandes, deberá asegurarse que las horas de los registros se encuentren coordinadas. Configure el host de referencia para utilizar el servidor NTP en su entorno que todos los hosts puedan compartir. Puede especificar un servidor NTP ejecutando el comando `esxcli system ntp set`. Puede iniciar y detener el servicio NTP para un host con el comando `esxcli system ntp set` o con vSphere Client.

Configuración del servidor de syslog

Todos los hosts ESXi ejecutan un servicio de Syslog (`vmsyslogd`), que registra mensajes desde VMkernel y otros componentes del sistema en un archivo. Puede especificar el host de registro y administrar la ubicación, la rotación, el tamaño y otros atributos del registro ejecutando el comando `esxcli system syslog` o a través de vSphere Client. La configuración de la generación de registros en un host remoto es especialmente importante para los hosts aprovisionados con vSphere Auto Deploy que no poseen almacenamiento local.

Opcionalmente, puede instalar VMware vCenter Log Insight, que proporciona análisis y agregación de registros.

Configuración de volcados de memoria

Puede configurar su host de referencia para enviar volcados de memoria a un LUN SAN compartido o puede instalar ESXi Dump Collector en su entorno y configurar el host de referencia para utilizar ESXi Dump Collector. Consulte Configurar ESXi Dump Collector con ESXCLI . Puede instalar ESXi Dump Collector a través del medio de instalación de vCenter Server o utilizar la instancia de ESXi Dump Collector que se incluye en vCenter Server. Después de que se complete la configuración, la memoria de VMkernel se envía al servidor de red especificado cuando el sistema encuentra un error crítico.

Configuración de seguridad

En la mayoría de las implementaciones, todos los hosts que aprovisione con vSphere Auto Deploy deberán tener la misma configuración de seguridad. Puede, por ejemplo, configurar el firewall para que permita el acceso de determinados servicios al sistema de ESXi, establecer la configuración de seguridad, la configuración de usuario y la configuración del grupo de usuarios para el host de referencia con los comandos ESXCLI o vSphere Client. La configuración de seguridad incluye la configuración compartida de acceso de usuarios para todos los hosts. Puede lograr un acceso de usuarios unificado mediante la configuración de su host de referencia para la utilización de Active Directory. Consulte la documentación sobre *seguridad de vSphere*.

Nota Si configura Active Directory utilizando perfiles de host, las contraseñas no poseen protección. Utilice vSphere Authentication Service para configurar Active Directory para evitar la exposición de la contraseña de Active Directory.

Configuración de conexión de redes y almacenamiento

Si reserva un conjunto de recursos de conexión de redes y almacenamiento para la utilización por parte de los hosts aprovisionados con vSphere Auto Deploy, puede configurar su host de referencia para utilizar dichos recursos.

En implementaciones grandes, la configuración del host de referencia admite un Enterprise Network Manager, que recolecta toda la información proveniente de diferentes servicios de supervisión que se ejecutan en su entorno.

Figura 4-9. Configurar el host de referencia con vSphere Auto Deploy

Opciones para la configuración de un host de referencia de vSphere Auto Deploy explica cómo realizar esta configuración.

Vea el vídeo Hosts de referencia con Auto Deploy para obtener información sobre la configuración del host de referencia:

 (Configurar los hosts de referencia con vSphere Auto Deploy)

Opciones para la configuración de un host de referencia de vSphere Auto Deploy

Puede configurar un host de referencia usando vSphere Client, ESXCLI o perfiles de host.

Para configurar un host de referencia, puede utilizar el enfoque que mejor se adapte a sus necesidades.

vSphere Client

vSphere Client admite la configuración de la conexión de red, almacenamiento, seguridad y muchos otros aspectos de un host ESXi. Configure su entorno y cree un perfil de host desde el host de referencia para su uso por parte de vSphere Auto Deploy.

ESXCLI

Puede usar ESXCLI para configurar varios aspectos del host. ESXCLI es adecuado para configurar muchos de los servicios en el entorno de vSphere. Los comandos son, entre otros, `esxcli system ntp` para configurar un servidor NTP, `esxcli system syslog` para configurar un servidor syslog, `esxcli network route` para agregar rutas y configurar la ruta predeterminada, y `esxcli system coredump` para configurar ESXi Dump Collector.

Función Perfiles de host

La práctica recomendada es configurar un host con vSphere Client o ESXCLI y crear un perfil de host desde dicho host. Si lo prefiere, no obstante, puede utilizar la función Perfiles de host en vSphere Client y guardar dicho perfil de host.

vSphere Auto Deploy aplica todas las configuraciones comunes del perfil de host a todos los hosts de destino. Si configura el perfil de host para solicitar la entrada del usuario, todos los hosts aprovisionados con dicho perfil de host aparecen en el modo de mantenimiento. Debe volver a aplicar el perfil de host o restablecer las personalizaciones del host para solicitar información específica del host.

Configurar un recopilador de volcado de ESXi

Puede configurar un ESXi Dump Collector para almacenar volcados de núcleo mediante comandos ESXCLI o configurando un host de referencia.

Los hosts aprovisionados con vSphere Auto Deploy no cuentan con un disco local en el que almacenar los volcados de núcleo. Puede configurar una instancia de ESXi Dump Collector para almacenar los volcados de núcleo mediante comandos ESXCLI o mediante la configuración de un host de referencia para usar ESXi Dump Collector mediante la función Perfiles de host de vSphere Client.

Configurar ESXi Dump Collector con ESXCLI

Los hosts aprovisionados con vSphere Auto Deploy no cuentan con un disco local para almacenar los volcados de memoria de núcleo. Puede configurar ESXi Dump Collector mediante

los comandos ESXCLI para mantener los volcados de núcleos en un servidor de red con la finalidad de usarlos durante las operaciones de depuración.

Un volcado de núcleo es el estado de la memoria de trabajo si se produce un error en el host. De forma predeterminada, los volcados de núcleos se guardan en el disco local. ESXi Dump Collector es especialmente útil para vSphere Auto Deploy, pero es compatible con cualquier host ESXi. ESXi Dump Collector admite otras opciones de personalización, incluido el envío de volcados de núcleos al disco local, y se incluye con el nodo de administración de vCenter Server.

Nota No es posible configurar ESXi Dump Collector en una interfaz de VMkernel que se ejecuta en un conmutador N-VDS de NSX-T.

Si va a usar IPv6 y el host ESXi y ESXi Dump Collector se encuentran en el mismo vínculo local, ambos pueden usar direcciones IPv6 de vínculo de alcance local o direcciones IPv6 de alcance global.

Si va a usar IPv6 y ESXi y ESXi Dump Collector se encuentran en hosts diferentes, ambos requieren direcciones IPv6 de alcance global. El tráfico se enruta por medio de la puerta de enlace IPv6 predeterminada.

Requisitos previos

Instale ESXCLI si quiere configurar el host para que use ESXi Dump Collector. En situaciones de solución de problemas, puede usar ESXCLI en ESXi Shell en su lugar.

Procedimiento

1 Configure un sistema ESXi para que use ESXi Dump Collector; para ello, ejecute `esxcli system coredump` en la instancia de ESXi Shell local o use ESXCLI.

```
 esxcli system coredump network set --interface-name vmk0    --server-ip 10xx.xx.xx.xx --
server-port 6500
```

   Debe especificar una dirección IP y la NIC de VMkernel, además de un puerto opcional del servidor al cual se deben enviar los volcados de núcleos. Puede usar una dirección IPv4 o IPv6. Si configura un sistema ESXi que se ejecuta en una máquina virtual que usa un conmutador estándar de vSphere, debe seleccionar un puerto de VMkernel que esté en modo promiscuo.

2 Habilite ESXi Dump Collector.

```
esxcli system coredump network set --enable true
```

3 (opcional) Compruebe que ESXi Dump Collector esté configurado correctamente.

```
esxcli system coredump network check
```

Resultados

El host en el que ha configurado ESXi Dump Collector está configurado para enviar los volcados de núcleos al servidor indicado mediante la NIC de VMkernel y el puerto opcional especificados.

Pasos siguientes

- Cree una regla que aplique el perfil de host a todos los hosts que desea aprovisionar con la configuración especificada en el host de referencia. Para escribir una regla en una sesión de PowerCLI, consulte Escribir una regla y asignar un perfil de host a hosts.
- Si los hosts ya se aprovisionaron con vSphere Auto Deploy, ejecute la prueba y repare las operaciones de cumplimiento en una sesión de PowerCLI. Para eso, consulte Probar y reparar cumplimiento de reglas .
- Encienda los hosts no aprovisionados para aprovisionarlos con el nuevo perfil de host.

Configurar ESXi Dump Collector desde la función de perfiles de host de vSphere Client

Los hosts aprovisionados con vSphere Auto Deploy no cuentan con un disco local para almacenar los volcados de memoria de núcleo. Puede configurar un host de referencia para usar ESXi Dump Collector desde la función de perfiles de host de vSphere Client.

La práctica recomendada es usar ESXi Dump Collector con el comando `esxcli system coredump` y guardar el perfil de host. Para obtener más información, consulte Configurar ESXi Dump Collector con ESXCLI .

Requisitos previos

- Compruebe que haya creado el perfil de host donde desea configurar una directiva de volcado de núcleo. Para obtener más información sobre la forma de crear un perfil de host, consulte la documentación de *Perfiles de host de vSphere*.
- Compruebe que al menos una partición disponga de capacidad de almacenamiento suficiente para los volcados de núcleos de varios hosts aprovisionados con vSphere Auto Deploy.

Procedimiento

1. Desplácese hasta **Inicio > Directivas y perfiles > Perfiles de host**.
2. Haga clic en el perfil de host que quiere configurar y seleccione la pestaña **Configurar**.
3. Haga clic en **Editar perfil de host**.
4. Seleccione **Configuración de redesConfiguración de volcados de núcleos de red**.
5. Active la casilla **Habilitado**.
6. Especifique la NIC del host que se debe usar, la IP del servidor de volcados de núcleos de red y el puerto del servidor de volcados de núcleos de red.
7. Haga clic en **Guardar** para completar la configuración del perfil de host.

Pasos siguientes

- Cree una regla que aplique el perfil de host a todos los hosts que desea aprovisionar con la configuración especificada en el host de referencia. Para escribir una regla en una sesión de PowerCLI, consulte Escribir una regla y asignar un perfil de host a hosts.
- Si los hosts ya se aprovisionaron con vSphere Auto Deploy, ejecute la prueba y repare las operaciones de cumplimiento en una sesión de PowerCLI. Para eso, consulte Probar y reparar cumplimiento de reglas .
- Encienda los hosts no aprovisionados para aprovisionarlos con el nuevo perfil de host.

Configurar Syslog desde perfiles de host de vSphere Client

Para especificar un servidor Syslog remoto, aplique un perfil de host.

La práctica recomendada es configurar el servidor syslog en el host de referencia con vSphere Client o con el comando `esxcli system syslog` y guardar el perfil de host. También puede configurar syslog desde la función de perfiles de host de vSphere Client.

Requisitos previos

Por lo general, los hosts aprovisionados con vSphere Auto Deploy no cuentan con almacenamiento local suficiente para guardar los registros del sistema. Puede especificar un servidor remoto de Syslog para esos hosts. Para ello, debe configurar un host de referencia, guardar el perfil de host y aplicar dicho perfil de host a los demás hosts según sea necesario.

- Si va a usar un host de Syslog remoto, configure ese host antes de personalizar los perfiles de host.
- Compruebe que tiene acceso a vSphere Client y al sistema vCenter Server.

Procedimiento

1. Desplácese hasta **Inicio > Directivas y perfiles > Perfiles de host**.
2. (opcional) Si no hay un host de referencia en el entorno, haga clic en **Extraer perfil de host** para crear un perfil de host.
3. Haga clic en el perfil de host que quiere configurar y seleccione la pestaña **Configurar**.
4. Haga clic en **Editar perfil de host**.
5. Seleccione **Opciones de configuración avanzadas > Opciones avanzadas > Opciones de configuración avanzadas**.

   Puede seleccionar subperfiles específicos y editar la configuración de syslog.
6. (opcional) Para crear una opción de configuración avanzada.
   a. Haga clic en el icono **Agregar subperfil**.
   b. Desde la lista desplegable **Opción avanzada**, seleccione **Configurar una opción fija**.
   c. Especifique *Syslog.global.loghost* como nombre de la opción y el host como valor de la opción.

7 Haga clic en **Guardar** para completar la configuración del perfil de host.

Pasos siguientes

- Cree una regla que aplique el perfil de host a todos los hosts que desea aprovisionar con la configuración especificada en el host de referencia. Para escribir una regla en una sesión de PowerCLI, consulte Escribir una regla y asignar un perfil de host a hosts.
- Si los hosts ya se aprovisionaron con vSphere Auto Deploy, ejecute la prueba y repare las operaciones de cumplimiento en una sesión de PowerCLI. Para eso, consulte Probar y reparar cumplimiento de reglas .
- Encienda los hosts no aprovisionados para aprovisionarlos con el nuevo perfil de host.

Habilitar el cliente NTP en un host de referencia de vSphere Client

Al recopilar información de generación de registros en entornos grandes, deberá asegurarse de que las horas de los registros se encuentren coordinadas.

Puede configurar el host de referencia para usar el servidor NTP en el entorno, extraer el perfil de host y crear una regla de vSphere Auto Deploy para aplicarla a los demás hosts.

Procedimiento

1 Desplácese hasta **Inicio > Hosts y clústeres**, y seleccione un host ESXi que quiera utilizar como host de referencia.

2 Seleccione la pestaña **Configurar**.

3 En **Sistema**, seleccione **Configuración de hora** y haga clic en **Editar**.

4 Seleccione el botón de opción **Usar protocolo de hora de red (Habilitar el cliente NTP)**.

Esta opción sincroniza la fecha y hora del host con un servidor NTP. El servicio NTP en el host toma periódicamente la fecha y la hora del servidor NTP.

5 Desde el menú desplegable **Directiva de inicio del servicio NTP**, seleccione **Iniciar y detener con el host**.

6 En el cuadro de texto **Servidores NTP**, escriba las direcciones IP o los nombres de host de los servidores NTP que desea usar.

7 Haga clic en **Aceptar**.

Pasos siguientes

- Extraiga un perfil de host del host de referencia. Consulte la documentación sobre *perfiles de host*.
- Cree una regla que aplique el perfil de host a todos los hosts que desea aprovisionar con la configuración especificada en el host de referencia. Para escribir una regla en una sesión de PowerCLI, consulte Escribir una regla y asignar un perfil de host a hosts.

Configurar las redes para los hosts vSphere Auto Deploy en vSphere Client

Puede configurar redes para el host de referencia de vSphere Auto Deploy y aplicar el perfil de host a todos los demás hosts a fin de garantizar un entorno de red completamente funcional.

Requisitos previos

Use vSphere Auto Deploy para aprovisionar el host que desea utilizar como host de referencia con una imagen de ESXi.

Procedimiento

1 Desplácese hasta **Inicio > Hosts y clústeres**, y seleccione un host ESXi que quiera utilizar como host de referencia.

2 Seleccione la pestaña **Configurar** y desplácese hasta **Redes**.

3 Realice la configuración de redes.

   Si usa conmutadores virtuales y no vSphere Distributed Switch, no agregue otras NIC de VMkernel a vSwitch0.

4 Después de configurar el host de referencia, reinicie el sistema para comprobar que vmk0 esté conectado a la red de administración.

5 Si no existen perfiles de host para su host de referencia, cree un perfil de host.

Pasos siguientes

- Cree una regla que aplique el perfil de host a todos los hosts que desea aprovisionar con la configuración especificada en el host de referencia. Para escribir una regla en una sesión de PowerCLI, consulte Escribir una regla y asignar un perfil de host a hosts.
- Si los hosts ya se aprovisionaron con vSphere Auto Deploy, ejecute la prueba y repare las operaciones de cumplimiento en una sesión de PowerCLI. Para eso, consulte Probar y reparar cumplimiento de reglas .
- Encienda los hosts no aprovisionados para aprovisionarlos con el nuevo perfil de host.

Configurar un host de referencia para la creación automática de particiones

Puede crear un host de referencia para crear particiones automáticamente de todos los hosts que aprovisione con vSphere Auto Deploy.

Precaución Si cambia el comportamiento predeterminado de creación automática de particiones, vSphere Auto Deploy sobrescribe las particiones existentes independientemente del contenido. Si activa esta opción, asegúrese de que no se produzca una pérdida de datos no intencionada.

A fin de garantizar que las unidades de estado sólido (SSD) locales permanezcan sin particionar durante la creación automática de particiones, deberá establecer el parámetro **`skipPartitioningSsds=TRUE`** en el host de referencia.

Para obtener más información sobre cómo evitar el formato de las unidades de estado sólido (SSD) durante la creación automática de particiones, consulte la documentación de *Almacenamiento de vSphere*.

Requisitos previos

De manera predeterminada, vSphere Auto Deploy aprovisiona los hosts solo si hay una partición disponible en el host. La opción de creación automática de particiones crea un almacén de datos de VMFS en el almacenamiento local del host. Puede configurar un host de referencia para crear particiones automáticamente de todos los hosts que aprovisione con vSphere Auto Deploy.

- Use vSphere Auto Deploy para aprovisionar el host que desea utilizar como host de referencia con una imagen de ESXi.
- Compruebe que tiene acceso a vSphere Client y que puede conectarse al sistema vCenter Server.

Procedimiento

1 Desplácese hasta **Inicio > Hosts y clústeres**, y seleccione un host ESXi que quiera utilizar como host de referencia.

2 Seleccione la pestaña **Configurar**.

3 En **Sistema**, seleccione **Configuración avanzada del sistema** y haga clic en **Editar**.

4 Busque la clave `VMkernel.Boot.autoPartition` y establezca el valor en **true**.

5 (opcional) Si desea que las unidades de estado sólido (SSD) locales permanezcan sin particionar, busque la clave `VMkernel.Boot.skipPartitioningSsds` y establezca el valor en **true**.

6 Haga clic en **Aceptar**.

7 Si no existen perfiles de host para su host de referencia, cree un perfil de host.

Resultados

La creación automática de particiones se realiza cuando se arrancan los hosts.

Pasos siguientes

- Utilice vSphere Auto Deploy para crear una regla que aplique el perfil de host de su host de referencia a todos los hosts inmediatamente al arrancar. Para crear una regla con vSphere Client, consulte Crear una regla de implementación. Para escribir una regla en una sesión de PowerCLI, consulte Escribir una regla y asignar un perfil de host a hosts.

Convertir hosts sin estado en hosts con estado

Puede agregar almacenamiento físico a su ESXi sin estado, convertirlos en hosts ESXi con estado y agregar los hosts a un clúster que administre mediante una imagen.

Los hosts ESXi deben tener un almacenamiento físico conectado, ya que un clúster administrado por una imagen no admite hosts ESXi sin estado, que usan un arranque de entorno de ejecución de prearranque (Preboot Execution Environment, PXE).

Para garantizar que los componentes de imagen se instalen en un disco físico de un host ESXi durante un proceso de arranque, Auto Deploy comprueba que un perfil de host forme parte de la imagen de arranque PXE. El perfil de host debe contener una directiva "Configuración de perfil de memoria caché de imagen del sistema" con la configuración establecida en "Habilitar instalaciones con estado en el host" o "Habilita instalaciones con estado en un disco USB en el host". Si el perfil de host asociado no contiene esta directiva o la configuración de la directiva es diferente, la directiva se configura automáticamente para admitir una instalación con estado. Si falta un perfil de host, se asocia un nuevo perfil de host al clúster, que contiene solo la directiva "Configuración de perfil de memoria caché de imagen del sistema" con una configuración para una instalación con estado.

Convertir un host ESXi sin disco

Para agregar hosts ESXi sin disco a un clúster administrado por una imagen, agregue almacenamiento físico, conviértalos en hosts con estado e instale una imagen de ESXi 8.0.

Para obtener información sobre el almacenamiento en caché sin estado y las instalaciones con estado, consulte Usar vSphere Auto Deploy para almacenamiento en caché sin estado e instalaciones con estado.

Requisitos previos

- Prepare el sistema e instale el servidor Auto Deploy. Para obtener más información, consulte *Preparar el sistema para vSphere Auto Deploy* en la documentación *Instalar y configurar VMware ESXi*.
- El host ESXi arranca a partir de una regla de Auto Deploy que contiene un perfil de imagen.
- El servicio Auto Deploy se está ejecutando.
- Tiene un stick USB vacío u otro almacenamiento compatible.

Procedimiento

1 En el menú Inicio, haga clic en **Directivas y perfiles** y seleccione **Perfiles de host**.

2 Extraiga un perfil de host de un host ESXi en ejecución o duplique un perfil de host existente con una configuración especificada y una ubicación de host.

   El perfil de host existente se puede asociar a un host o a un clúster.

3 Haga clic con el botón derecho en el nuevo perfil de host, seleccione **Editar perfil de host** y desplácese hasta **Opciones de configuración avanzadas > Configuración de memoria caché de imagen del sistema > Configuración de memoria caché de imagen del sistema**.

4 En el menú desplegable **Configuración de perfil de memoria caché de imagen del sistema**, elija una opción de directiva.

Opción	Descripción
Habilitar almacenamiento en caché sin estado en el host	Almacena en caché la imagen en el disco.
Habilitar almacenamiento en caché sin estado en un disco USB del host	Almacena en caché la imagen en un disco USB asociado al host.

5 En función de la opción de directiva que seleccione, debe hacer lo siguiente:

   a Si selecciona **Habilitar almacenamiento en caché sin estado en el host**:

      1 Introduzca argumentos para el primer disco y seleccione las casillas si es necesario.

      2 En el menú desplegable **Configuración de disco del sistema**, seleccione **Elección explícita de la opción de directiva por parte del usuario**.

   b Si selecciona **Habilitar almacenamiento en caché sin estado en un disco USB del host**:

      1 En el menú desplegable **Configuración de disco del sistema**, seleccione **Disco del sistema especificado por el usuario en la personalización del host**.

      2 En **Hosts y clústeres**, haga clic con el botón derecho en el host y seleccione **Perfiles de host > Editar personalizaciones de host**. Defina un disco con almacenamiento persistente en el campo **Valor** para la propiedad **Disco del sistema**.

6 Haga clic en **Guardar** para completar la configuración del perfil de host.

7 Si duplicó un perfil de host existente y dicho perfil estaba asociado a un clúster, asocie el nuevo perfil de host al clúster en cuestión.

8 En el menú Inicio, haga clic en **Auto Deploy**.

9 Desactive la regla de Auto Deploy que contiene un perfil de imagen y haga clic en **Editar**.

   Se mostrará el cuadro de diálogo Editar regla de implementación.

10 En la página **Seleccionar perfil de imagen** del asistente, seleccione un perfil de imagen de ESXi 8.0.

11 En la página **Seleccionar perfil de host** del asistente, seleccione un nuevo perfil de host.

12 Active la regla y muévala a la posición inicial de la regla en la lista ordenada.

13 En la pestaña **Hosts implementados**, seleccione uno o varios hosts ESXi.

14 Haga clic en la opción **Corregir asociaciones de hosts** relativa al host ESXi.

Puede supervisar el progreso del proceso de corrección en el panel Tareas recientes.

15 Apague los hosts ESXi corregidos.

16 Una vez que los hosts ESXi estén apagados, instale el almacenamiento seleccionado como discos de arranque local.

17 Encienda cada host ESXi, introduzca la configuración de BIOS/UEFI y cambie el orden de arranque para que arranque primero desde el almacenamiento recién agregado y, a continuación, desde la red.

Dado que el almacenamiento recién agregado está vacío, cada host ESXi arranca desde la red e instala la imagen de ESXi 8.0 que especificó anteriormente en el almacenamiento. Después de la instalación, cada host ESXi se reinicia y arranca desde el almacenamiento recién agregado.

Resultados

Los hosts ESXi arrancan de forma predeterminada desde el nuevo almacenamiento y funcionan como si la imagen de ESXi 8.0 hubiera instalado desde un DVD estándar.

Pasos siguientes

Agregue los hosts ESXi a un clúster que administre mediante una sola imagen. Para obtener más información, consulte *Agregar un host* en la documentación de *Administrar vCenter Server y hosts*.

Convertir un host ESXi sin estado con almacenamiento en caché sin estado habilitado

Para agregar los hosts ESXi sin estado a un clúster que administre mediante una imagen, primero debe convertir los hosts en hosts con estado mediante la instalación de una imagen de 8.0 8.0 estándar.

Para obtener información sobre el almacenamiento en caché sin estado y las instalaciones con estado, consulte Usar vSphere Auto Deploy para almacenamiento en caché sin estado e instalaciones con estado.

Requisitos previos

- Prepare el sistema e instale el servidor Auto Deploy. Para obtener más información, consulte *Preparar el sistema para vSphere Auto Deploy* en la documentación *Instalar y configurar VMware ESXi*.
- El host ESXi arranca a partir de una regla de Auto Deploy que contiene un perfil de imagen.
- El servicio Auto Deploy se está ejecutando.

Procedimiento

1 En el menú Inicio, haga clic en **Directivas y perfiles** y seleccione **Perfiles de host**.

2 Extraiga un perfil de host de un host ESXi en ejecución o duplique un perfil de host existente con una configuración especificada y una ubicación de host.

   El perfil de host existente se puede asociar a un host o a un clúster.

3 Haga clic con el botón derecho en el nuevo perfil de host, seleccione **Editar perfil de host** y desplácese hasta **Opciones de configuración avanzadas > Configuración de memoria caché de imagen del sistema > Configuración de memoria caché de imagen del sistema**.

4 Seleccione **Habilitar instalaciones con estado en el host** en el menú desplegable, introduzca `local` en el cuadro de texto **Argumentos para el primer disco** y active la casilla **Marcar para sobrescribir los volúmenes VMFS en el disco seleccionado**.

5 Si duplicó un perfil de host existente y dicho perfil estaba asociado a un clúster, asocie el nuevo perfil de host al clúster en cuestión.

6 En el menú Inicio, haga clic en **Auto Deploy**.

7 Desactive la regla de Auto Deploy que contiene un perfil de imagen y haga clic en **Editar**.

   Se mostrará el cuadro de diálogo Editar regla de implementación.

8 En la página **Seleccionar perfil de imagen** del asistente, seleccione un perfil de imagen de ESXi 8.0.

9 En la página **Seleccionar perfil de host** del asistente, seleccione un nuevo perfil de host.

10 Active la regla y muévala a la posición inicial de la regla en la lista ordenada.

11 En la pestaña **Hosts implementados**, seleccione uno o varios hosts ESXi.

12 Haga clic en la opción **Corregir asociaciones de hosts** relativa al host ESXi.

   Puede supervisar el progreso del proceso de corrección en el panel Tareas recientes.

13 Reinicie los hosts ESXi.

   Si un host ESXi tiene un BIOS heredado, puede cambiar el orden de arranque en la configuración del BIOS para que arranque primero desde el almacenamiento local. Para los hosts ESXi basados en UEFI, el orden de arranque cambia automáticamente durante el reinicio.

   Cada host ESXi arranca desde la red e instala la imagen de ESXi 8.0 que especificó más arriba en el almacenamiento utilizado anteriormente para el almacenamiento en caché. Después de la instalación, cada host ESXi se reinicia de nuevo y arranca desde el almacenamiento local.

Resultados

Los hosts ESXi arrancan de forma predeterminada desde el nuevo almacenamiento y funcionan como si la imagen de ESXi 8.0 hubiera instalado desde un DVD estándar.

Pasos siguientes

Agregue los hosts ESXi a un clúster que administre mediante una sola imagen. Para obtener más información, consulte *Agregar un host* en la documentación de *Administrar vCenter Server y hosts*.

Convertir un host ESXi sin estado con una única partición de VMFS en el disco local

Para agregar los hosts ESXi sin estado a un clúster que administre mediante una imagen, primero debe convertir los hosts en hosts con estado volviendo a particionar las particiones de VMFS e instalando una imagen de ESXi 8.0 estándar.

Para obtener información sobre el almacenamiento en caché sin estado y las instalaciones con estado, consulte Usar vSphere Auto Deploy para almacenamiento en caché sin estado e instalaciones con estado.

Requisitos previos

- Prepare el sistema e instale el servidor Auto Deploy. Para obtener más información, consulte *Preparar el sistema para vSphere Auto Deploy* en la documentación *Instalar y configurar VMware ESXi*.
- El host ESXi arranca a partir de una regla de Auto Deploy que contiene un perfil de imagen.
- El servicio Auto Deploy se está ejecutando.

Procedimiento

1 En el menú Inicio, haga clic en **Directivas y perfiles** y seleccione **Perfiles de host**.

2 Extraiga un perfil de host de un host ESXi en ejecución o duplique un perfil de host existente con una configuración especificada y una ubicación de host.

   El perfil de host existente se puede asociar a un host o a un clúster.

3 Haga clic con el botón derecho en el nuevo perfil de host, seleccione **Editar perfil de host** y desplácese hasta **Opciones de configuración avanzadas > Configuración de memoria caché de imagen del sistema > Configuración de memoria caché de imagen del sistema**.

4 Seleccione **Habilitar instalaciones con estado en el host** en el menú desplegable e introduzca `localesx` en el cuadro de texto **Argumentos para el primer disco**.

5 Si duplicó un perfil de host existente y dicho perfil estaba asociado a un clúster, asocie el nuevo perfil de host al clúster en cuestión.

6 En el menú Inicio, haga clic en **Auto Deploy**.

7 Desactive la regla de Auto Deploy que contiene un perfil de imagen y haga clic en **Editar**.

   Se mostrará el cuadro de diálogo Editar regla de implementación.

8 En la página **Seleccionar perfil de imagen** del asistente, seleccione un perfil de imagen de ESXi 8.0.

9 En la página **Seleccionar perfil de host** del asistente, seleccione un nuevo perfil de host.

10 Active la regla y muévala a la posición inicial de la regla en la lista ordenada.

11 En la pestaña **Hosts implementados**, seleccione uno o varios hosts ESXi.

12 Haga clic en la opción **Corregir asociaciones de hosts** relativa al host ESXi.

Puede supervisar el progreso del proceso de corrección en el panel Tareas recientes.

13 Reinicie los hosts ESXi.

Si un host ESXi tiene un BIOS heredado, puede cambiar el orden de arranque en la configuración del BIOS para que arranque primero desde el almacenamiento local. Para los hosts ESXi basados en UEFI, el orden de arranque cambia automáticamente durante el reinicio.

Cada host ESXi arranca desde la red, vuelve a particionar la partición de VMFS en una partición de instalación de ESXi estándar e instala la imagen de ESXi 8.0 que especificó anteriormente en la partición. Después de la instalación, cada host ESXi se reinicia de nuevo y arranca desde la partición de ESXi estándar.

Resultados

Los hosts ESXi arrancan de forma predeterminada desde la nueva partición y funcionan como si la imagen de ESXi 8.0 se hubiera instalado desde un DVD estándar.

Pasos siguientes

Agregue los hosts ESXi a un clúster que administre mediante una sola imagen. Para obtener más información, consulte *Agregar un host* en la documentación de *Administrar vCenter Server y hosts*.

Convertir un host ESXi sin estado con una única partición de VMFS en un disco remoto

Para agregar los hosts ESXi sin estado a un clúster que administre mediante una imagen, primero debe convertir los hosts en hosts con estado volviendo a particionar las particiones de VMFS remotas e instalando una imagen de ESXi 8.0 estándar. Por ejemplo el host ESXi puede arrancar desde SAN de canal de fibra o desde SAN de iSCSI.

Para obtener información sobre el almacenamiento en caché sin estado y las instalaciones con estado, consulte Usar vSphere Auto Deploy para almacenamiento en caché sin estado e instalaciones con estado.

Para obtener más información sobre el arranque desde un disco remoto, consulte *Arrancar desde SAN iSCSI* en la documentación de *Almacenamiento de vSphere*.

Requisitos previos

- Prepare el sistema e instale el servidor Auto Deploy. Para obtener más información, consulte *Preparar el sistema para vSphere Auto Deploy* en la documentación *Instalar y configurar VMware ESXi*.
- El host ESXi arranca a partir de una regla de Auto Deploy que contiene un perfil de imagen.
- El servicio Auto Deploy se está ejecutando.

Procedimiento

1. En el menú Inicio, haga clic en **Directivas y perfiles** y seleccione **Perfiles de host**.
2. Extraiga un perfil de host de un host ESXi en ejecución o duplique un perfil de host existente con una configuración especificada y una ubicación de host.

   El perfil de host existente se puede asociar a un host o a un clúster.
3. Haga clic con el botón derecho en el nuevo perfil de host, seleccione **Editar perfil de host** y desplácese hasta **Opciones de configuración avanzadas > Configuración de memoria caché de imagen del sistema > Configuración de memoria caché de imagen del sistema**.
4. Seleccione **Habilitar instalaciones con estado en el host** en el menú desplegable e introduzca `remoteesx,remote` o `sortedremoteesx,sortedremote` en el cuadro de texto **Argumentos para el primer disco**.
5. Si duplicó un perfil de host existente y dicho perfil estaba asociado a un clúster, asocie el nuevo perfil de host al clúster en cuestión.
6. En el menú Inicio, haga clic en **Auto Deploy**.
7. Desactive la regla de Auto Deploy que contiene un perfil de imagen y haga clic en **Editar**.

   Se mostrará el cuadro de diálogo Editar regla de implementación.
8. En la página **Seleccionar perfil de imagen** del asistente, seleccione un perfil de imagen de ESXi 8.0.
9. En la página **Seleccionar perfil de host** del asistente, seleccione un nuevo perfil de host.
10. Active la regla y muévala a la posición inicial de la regla en la lista ordenada.
11. En la pestaña **Hosts implementados**, seleccione uno o varios hosts ESXi.
12. Haga clic en la opción **Corregir asociaciones de hosts** relativa al host ESXi.

    Puede supervisar el progreso del proceso de corrección en el panel Tareas recientes.
13. Reinicie los hosts ESXi.

    Cada host ESXi arranca desde la red, vuelve a particionar la partición de VMFS en una partición de instalación de ESXi estándar e instala la imagen de ESXi 8.0 que especificó anteriormente en la partición. Después de la instalación, cada host ESXi se reinicia de nuevo y arranca desde la partición de ESXi estándar remota.

Resultados

Los hosts ESXi arrancan de forma predeterminada desde la nueva partición y funcionan como si la imagen de ESXi 8.0 se hubiera instalado desde un DVD estándar.

Pasos siguientes

Agregue los hosts ESXi a un clúster que administre mediante una sola imagen. Para obtener más información, consulte *Agregar un host* en la documentación de *Administrar vCenter Server y hosts*.

Prácticas recomendadas de vSphere Auto Deploy

Configure la infraestructura altamente disponible de vSphere Auto Deploy en entornos de producción de gran tamaño o cuando utilice almacenamiento en caché sin estado.

Siga las prácticas recomendadas al instalar vSphere Auto Deploy y al utilizar vSphere Auto Deploy con otros componentes de vSphere. Configure la infraestructura altamente disponible de vSphere Auto Deploy en entornos de producción de gran tamaño o cuando utilice almacenamiento en caché sin estado. Siga todas las instrucciones de seguridad que seguiría en un entorno de arranque PXE y tenga en cuenta las recomendaciones de este capítulo.

Prácticas recomendadas de vSphere Auto Deploy

Siga las prácticas recomendadas de vSphere Auto Deploy para configurar redes, configurar vSphere HA y optimizar el entorno para vSphere Auto Deploy.

Consulte la base de conocimientos de VMware para obtener más información sobre las prácticas recomendadas.

Prácticas recomendadas de vSphere HA y vSphere Auto Deploy

Siga las prácticas recomendadas para mejorar la disponibilidad de las máquinas virtuales que se ejecutan en los hosts aprovisionados con vSphere Auto Deploy.

En algunos entornos se configuran los hosts aprovisionados con vSphere Auto Deploy con un conmutador distribuido o se configuran las máquinas virtuales que se ejecutan en los hosts con Auto Start Manager. En este tipo de entornos, implemente el sistema vCenter Server de manera que su disponibilidad coincida con la disponibilidad del servidor vSphere Auto Deploy. Se pueden emplear diversos métodos.

- Implementar vCenter Server. Se incluye el servidor vSphere Auto Deploy.
- Ejecute vCenter Server en un clúster habilitado para vSphere HA y configure la máquina virtual con una prioridad de reinicio de vSphere HA alta. Incluya dos o más hosts en el clúster que no estén administrados por vSphere Auto Deploy y ancle la máquina virtual de vCenter Server a estos hosts mediante una regla (vSphere HA DRS requiere la regla basada en el anclaje de máquina virtual a hosts). Puede configurar la regla y después desactivar DRS si no desea usar DRS en el clúster. Cuanto mayor sea la cantidad de hosts no administrados por vSphere Auto Deploy, mayor será la resistencia a errores del host.

  Nota Este método no resulta adecuado si se usa Auto Start Manager. Auto Start Manager no es compatible en un clúster habilitado para vSphere HA.

Prácticas recomendadas de red de vSphere Auto Deploy

Siga las prácticas recomendadas de red de vSphere Auto Deploy para prevenir problemas de red.

vSphere Auto Deploy e IPv6

Dado que vSphere Auto Deploy aprovecha la infraestructura de iPXE, si los hosts que desea aprovisionar con vSphere Auto Deploy usan BIOS heredado, el servidor vSphere Auto Deploy

debe tener una dirección IPv4. El arranque PXE con firmware de BIOS heredado solo se puede realizar mediante IPv4. El arranque PXE con firmware UEFI se puede realizar mediante IPv4 o IPv6.

Asignación de direcciones IP

Use las reservas de DHCP para la asignación de direcciones. El mecanismo de personalización de hosts admite direcciones IP fijas, pero no se recomienda proporcionar entradas para cada host.

Consideraciones sobre las VLAN

Use vSphere Auto Deploy en los entornos que no emplean VLAN.

Si va a usar vSphere Auto Deploy en un entorno que emplea VLAN, asegúrese de que los hosts que desea aprovisionar puedan comunicarse con el servidor DHCP. La manera en que se asignan los hosts a una VLAN depende de la configuración del sitio. El conmutador o el enrutador pueden asignar el identificador de la VLAN, o bien puede configurarse en el BIOS del host o mediante el perfil de host. Póngase en contacto con su administrador de red a fin de determinar los pasos para permitir que los hosts se comuniquen con el servidor DHCP.

Prácticas recomendadas de VMware Tools y vSphere Auto Deploy

Al aprovisionar hosts con vSphere Auto Deploy, es posible seleccionar un perfil de imagen que incluya VMware Tools o seleccionar la imagen más pequeña asociada con el perfil de imagen que no contenga VMware Tools.

Puede descargar dos perfiles de imagen desde el sitio de descargas de VMware.

- `*xxxxx*-standard`: un perfil de imagen que incluye los archivos binarios de VMware Tools, necesarios para el sistema operativo invitado que se ejecuta dentro de una máquina virtual. Generalmente, la imagen tiene el nombre esxi-*version*-*xxxxx*-standard.
- `*xxxxx*-no-tools`: un perfil de imagen que no incluye los archivos binarios de VMware Tools. Generalmente, este perfil de imagen es más pequeño y tiene una menor sobrecarga de memoria, y se arranca más rápidamente en un entorno de arranque con PXE. Generalmente, esta imagen tiene el nombre esxi-*version*-*xxxxx*-no-tools.

Puede implementar ESXi mediante cualquiera de los perfiles de imagen.

- Si el tiempo de arranque de la red no es un factor importante, y el entorno dispone de memoria adicional y sobrecarga de almacenamiento suficientes, use la imagen que incluye VMware Tools.
- Si considera que el tiempo de arranque de la red se extiende demasiado al usar la imagen estándar, o si desea ahorrar espacio en los hosts, puede usar el perfil de imagen que no incluye VMware Tools y colocar los archivos binarios de VMware Tools en almacenamiento compartido. Consulte Aprovisionar hosts ESXi mediante un perfil de imagen sin VMware Tools.

Prácticas recomendadas de administración de cargas de vSphere Auto Deploy

El arranque simultáneo de grandes cantidades de hosts supone una carga considerable para el servidor vSphere Auto Deploy. Debido a que, en esencia, vSphere Auto Deploy es un servidor web, puede usar las tecnologías existentes de escala de servidores web para ayudar a distribuir la carga. Por ejemplo, con vSphere Auto Deploy se pueden usar uno o más servidores proxy inversos de almacenamiento en caché. Los servidores proxy inversos proporcionan los archivos estáticos que constituyen la mayor parte de una imagen de arranque de ESXi. Configure el proxy inverso para que almacene en caché el contenido estático y para que transmita todas las solicitudes por medio del servidor vSphere Auto Deploy. Para obtener más información, vea el vídeo sobre el uso de servidores proxy web inversos para el escalado de vSphere Auto Deploy:

 (Uso de servidores proxy web inversos para el escalado de vSphere Auto Deploy)

Use varios servidores TFTP para apuntar a diferentes servidores proxy. Use un servidor TFTP para cada servidor proxy inverso. A continuación, configure el servidor DHCP para que envíe diferentes hosts a diferentes servidores TFTP.

Al arrancar los hosts, el servidor DHCP los redirige a diferentes servidores TFTP. Cada servidor TFTP redirige los hosts a un servidor diferente, ya sean el servidor vSphere Auto Deploy o un servidor proxy inverso, lo que reduce de manera sustancial la carga en el servidor vSphere Auto Deploy.

Después de una interrupción de alimentación masiva, vuelva a encender los hosts respetando el orden de cada clúster. Si conecta varios clústeres de forma simultánea, es posible que el servidor vSphere Auto Deploy experimente cuellos de botella de CPU. Todos los hosts se conectan después de una demora. El cuello de botella es menos severo si se configura el proxy inverso.

Prácticas recomendadas de registro y solución de problemas de vSphere Auto Deploy

Con la finalidad de solucionar los problemas experimentados con vSphere Auto Deploy, use la información de registro de vSphere Auto Deploy disponible en vSphere Client y configure el entorno para que envíe la información de registro y los volcados de memoria de núcleo a los hosts remotos.

Registros de vSphere Auto Deploy

Descargue los registros de vSphere Auto Deploy desde la página de vSphere Auto Deploy en vSphere Client. Consulte Descargar registros de vSphere Auto Deploy.

Configuración de Syslog

Configure un servidor remoto de Syslog. Consulte la documentación de *Administrar vCenter Server y hosts* para obtener información sobre la configuración del servidor de Syslog. Configure el primer host que arranque para que use el servidor remoto de Syslog y aplique el perfil de host de dicho host a todos los demás hosts de destino. Opcionalmente, puede instalar y usar vSphere Syslog Collector, una herramienta de apoyo de vCenter Server que

proporciona una arquitectura unificada para el registro de sistema, permite el registro de red y permite combinar registros de diversos hosts.

Configuración de ESXi Dump Collector

Los hosts aprovisionados con vSphere Auto Deploy no cuentan con un disco local para almacenar los volcados de memoria de núcleo. Instale ESXi Dump Collector y configure el primer host para que todos los volcados de memoria de núcleos se envíen a ESXi Dump Collector y aplique el perfil de host de dicho host a todos los demás hosts. Consulte Configurar ESXi Dump Collector con ESXCLI .

Usar vSphere Auto Deploy en un entorno de producción

Al cambiar de una configuración de prueba de concepto a un entorno de producción, asegúrese de que el entorno sea resistente.

- Proteja el servidor vSphere Auto Deploy. Consulte Prácticas recomendadas de vSphere HA y vSphere Auto Deploy.
- Proteja todos los demás servidores del entorno, incluidos el servidor DHCP y el servidor TFTP.
- Siga las directrices de seguridad de VMware, incluidas las que se detallan en Consideraciones de seguridad de vSphere Auto Deploy.

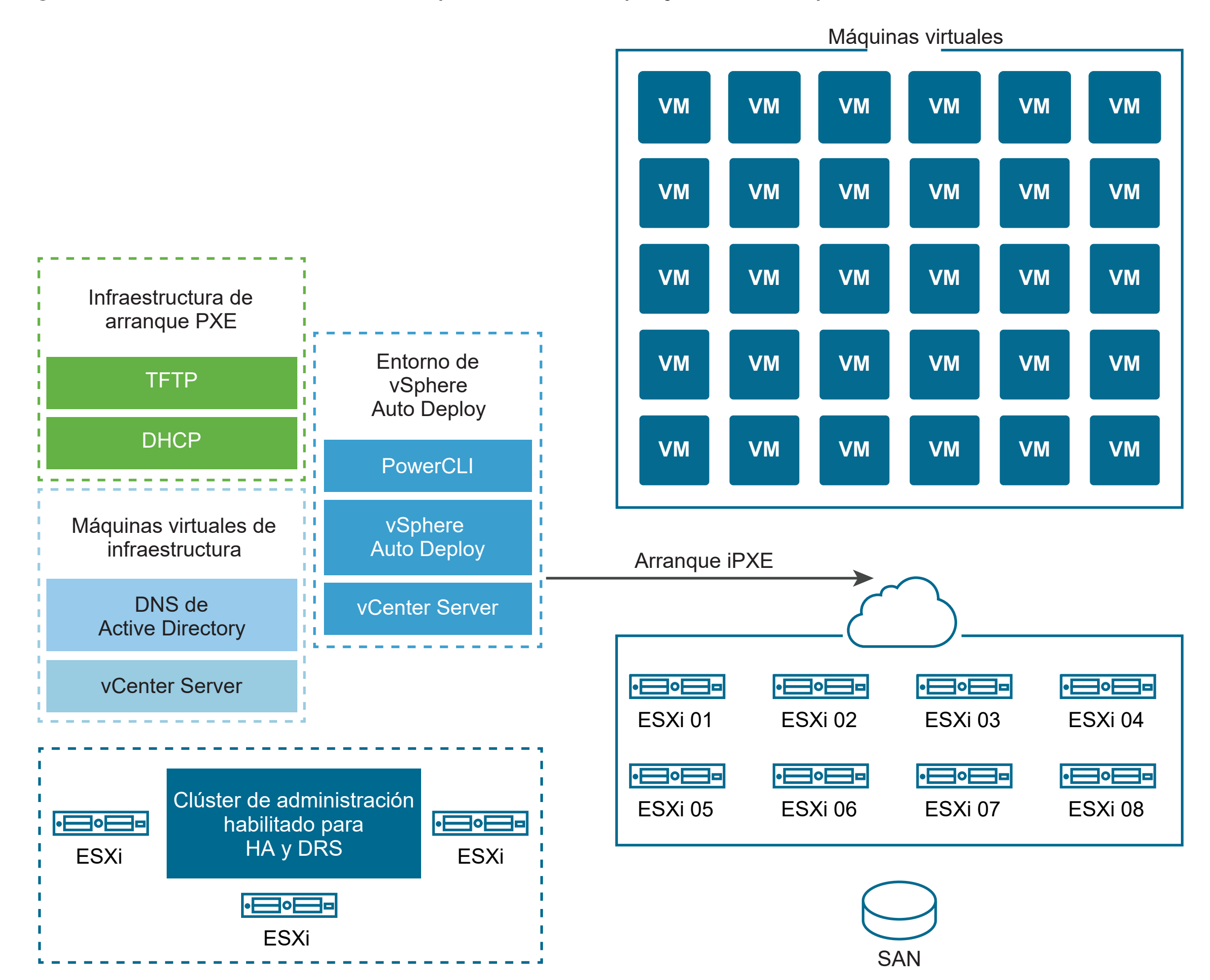
Configurar la infraestructura de vSphere Auto Deploy de alta disponibilidad

La infraestructura de vSphere Auto Deploy de alta disponibilidad evita la pérdida de datos y es un requisito previo para usar vSphere Auto Deploy con almacenamiento en caché sin estado.



(Infraestructura de vSphere Auto Deploy de alta disponibilidad)

Figura 4-10. Infraestructura de vSphere Auto Deploy de alta disponibilidad



Requisitos previos

En muchas situaciones de producción, se necesita una infraestructura de vSphere Auto Deploy de alta disponibilidad para evitar la pérdida de datos. Esta infraestructura también es uno de los requisitos previos para usar vSphere Auto Deploy con almacenamiento en caché sin estado.

Para el clúster de administración, instale ESXi en tres hosts. No aprovisione los hosts del clúster de administración con vSphere Auto Deploy.

Mire el vídeo "Highly Available vSphere Auto Deploy Infrastructure" para obtener información sobre la implementación de una infraestructura de vSphere Auto Deploy de alta disponibilidad:

Procedimiento

1 Habilite vSphere HA y vSphere DRS en el clúster de administración.

2 Configure las siguientes máquinas virtuales en el clúster de administración.

Componente de infraestructura	Descripción
Infraestructura de arranque PXE	Servidores de DHCP y TFTP.
Máquina virtual de infraestructura	Active Directory, DNS, vCenter Server.
Entorno de vSphere Auto Deploy	PowerCLI, servidor vSphere Auto Deploy, vCenter Server. Configure este entorno en una sola máquina virtual o en tres máquinas virtuales independientes en los sistemas de producción.

vCenter Server en la máquina virtual de infraestructura es diferente a vCenter Server en el entorno de vSphere Auto Deploy.

3 Configure vSphere Auto Deploy para aprovisionar otros hosts según sea necesario.

Debido a que los componentes del clúster de administración están protegidos mediante vSphere HA, la característica de alta disponibilidad es compatible.

Consideraciones de seguridad de vSphere Auto Deploy

Cuando utilice vSphere Auto Deploy, preste especial atención a la seguridad de redes, a la seguridad de la imagen de arranque y a la posible exposición de la contraseña para proteger su entorno.

Seguridad de redes

Asegure su red igual que si se tratara de cualquier otro método de implementación basado en PXE. vSphere Auto Deploy transfiere datos por SSL para evitar interferencias accidentales e intromisiones. Sin embargo, la autenticidad del cliente o del servidor Auto Deploy no se comprueba durante un arranque PXE.

Puede reducir ampliamente el riesgo de seguridad de Auto Deploy aislando por completo la red donde se utiliza Auto Deploy.

Imagen de arranque y seguridad de perfil de host

La imagen de arranque que descarga el servidor vSphere Auto Deploy en una máquina puede tener los siguientes componentes.

- Los paquetes de VIB que componen el perfil de imagen se incluyen siempre en la imagen de arranque.
- El perfil de host y la personalización del host se incluyen en la imagen de arranque si las reglas de Auto Deploy se configuran para aprovisionar el host con un perfil o una personalización del host.
  - La contraseña de administrador (raíz) y las contraseñas de usuario que se incluyen en el perfil de host y en la personalización de host están cifradas con hash SHA-512.
  - Cualquier otra contraseña asociada a los perfiles quedará excluida. Si configura Active Directory utilizando perfiles de host, las contraseñas no poseen protección.

Utilice vSphere Authentication Proxy para evitar la exposición de las contraseñas de Active Directory. Si configura Active Directory utilizando perfiles de host, las contraseñas no están protegidas.

- El certificado y la clave SSL públicas y privadas del host se incluyen en la imagen de arranque.

Configuración de alias de dispositivo.

Los alias de dispositivos, también conocidos como nombres de dispositivos, son nombres cortos asociados a los adaptadores de E/S en un subsistema de E/S.

Por ejemplo, los vínculos superiores de red tienen alias como vmnic0, vmnic1, etc. Los objetos del adaptador de SCSI de los objetos del dispositivo de gráficos y el subsistema de almacenamiento también tienen alias. Un dispositivo de hardware se puede presentar como varios adaptadores de E/S en el subsistema de E/S. Los adaptadores de E/S pueden ser de un tipo diferente al del dispositivo físico subyacente. Por ejemplo, un dispositivo FCoE es un adaptador de E/S de almacenamiento que utiliza el hardware de la NIC. El iSCSI de software es un adaptador de almacenamiento que utiliza la pila de red en la capa de IP. Por lo tanto, en el modelo de controlador nativo de ESXi, los alias solo suelen hacer referencia a los adaptadores de E/S y no a los dispositivos físicos, como una NIC de PCI o un HBA de PCI.

Asignación de alias de dispositivo

Un modelo de implementación de ESXi sin estado es aquel en el que el host ESXi no está instalado en discos duros y, por lo general, se arranca mediante PXE. Un modelo de implementación de ESXi con estado es aquel en el que el host ESXi se instala en los discos duros locales. La asignación de alias de dispositivo se produce durante un arranque de ESXi sin estado o una instalación nueva de ESXi con estado. El host ESXi asigna los alias a los adaptadores de E/S en un orden basado en el orden de enumeración del hardware subyacente. El host ESXi asigna primero los alias a los dispositivos integrados y, a continuación, a las tarjetas complementarias según el orden de la ranura. El host ESXi no puede asignar alias a dispositivos ausentes o dispositivos sin controladores compatibles.

Un vínculo superior que utiliza una NIC integrada en la placa base recibe un alias vmnicN con un número inferior que el que recibe un vínculo superior de una tarjeta de complemento PCI. Es posible que el controlador de la NIC registre más de un vínculo superior. Si uno de los vínculos superiores no corresponde a un dispositivo de hardware enumerable, el host ESXi asigna el siguiente alias disponible al vínculo superior después de que el vínculo superior se registre en el sistema.

Persistencia de la configuración de alias de dispositivo

Una vez que el host ESXi asigna los alias, se conserva la configuración de alias. El host ESXi intenta mantener el alias de cada dispositivo igual, independientemente de las actualizaciones de la versión de ESXi o de los cambios de hardware, como la adición o eliminación de los dispositivos de las ranuras.

La persistencia de la configuración de alias depende del modelo de implementación.

- En los sistemas con estado, la configuración de alias se conserva localmente en el host.

- En los sistemas sin estado, si no administra el sistema sin estado mediante perfiles de host, la configuración de alias no se conservará localmente en el host.
- En los sistemas con estado y sin estado que se administran mediante perfiles de host, la configuración de alias se conserva en el perfil del host. Si aplica un perfil de host a un host con estado, el perfil del host reemplaza cualquier configuración de alias persistente en local.

Cambios en la configuración de alias de dispositivo

La persistencia de la configuración de alias se basa en las direcciones de bus de los dispositivos. Si se modifica la dirección de bus de un dispositivo, la configuración de alias persistente deja de poder aplicarse y los alias asignados al dispositivo podrían cambiar.

Los cambios en la configuración de alias de dispositivo pueden producirse en los siguientes casos:

- La actualización de un controlador puede enumerar o presentar un adaptador de E/S diferente al sistema en comparación con el modo en que se presenta el adaptador de E/S antes de la actualización del controlador.
- Una actualización de pila puede provocar cambios en partes de una configuración de controlador de varios módulos o en la pila de E/S de ESXi que admite un controlador de varios módulos.
- Las actualizaciones de BIOS o de firmware de dispositivo pueden producir información incompleta de ranura o puerto.
- Cambios en la posición de ranura de un dispositivo.

Nota Si elimina un dispositivo del sistema, se elimina también la configuración de alias de los adaptadores de E/S del dispositivo. Si vuelve a agregar los mismos dispositivos al sistema más adelante, es posible que los adaptadores de E/S del dispositivo no reciban sus alias anteriores.

Configuración de alias de dispositivo en clústeres de ESXi

La configuración del alias inicial es la misma en un clúster de sistemas idénticos. Sin embargo, incluso en un clúster que se considera homogéneo, las pequeñas diferencias que existen en el hardware o el firmware pueden provocar diferencias en la configuración de alias entre hosts.

Las diferencias en el orden de procesamiento durante el enlace de controladores también pueden provocar diferencias en la configuración de alias. Por ejemplo, un controlador de NIC registra dos vínculos superiores (uplink-1 y uplink-2) para dos puertos del mismo dispositivo PCI, donde uno de los puertos no es un hardware enumerable por el sistema. Los cambios de tiempo en el orden de registro de los vínculos superiores pueden provocar diferencias en el modo en que los hosts ESXi asignan alias a los vínculos superiores. Un host ESXi puede asignar el alias basado en hardware al vínculo superior 1 (uplink-1) y otro host ESXi puede asignar el alias basado en hardware al vínculo superior 2 (uplink-2).

Para que coincida la configuración de alias en los hosts homogéneos, puede utilizar perfiles de host. El perfil de host de configuración de alias de dispositivo aplica la configuración de alias a un host ESXi mediante la asignación de los dispositivos en la configuración de alias a los dispositivos de host ESXi. La operación de asignación se basa en las fuentes de información del hardware que se utilizan como base para la asignación de alias inicial. Para obtener más información sobre los orígenes de información que se utilizan para asignar los alias, consulte el artículo de la base de conocimientos KB 2091560.

El perfil de host de configuración de alias de dispositivo también marca errores; por ejemplo, cuando un dispositivo está presente en el perfil de host pero no lo está en el host.

Un clúster heterogéneo no tiene la misma configuración de alias predeterminada en sus hosts. Debido a las diferencias entre los dispositivos, un perfil de host no se puede aplicar correctamente.

Usar los comandos de ESXi Shell para ver la información de alias de un dispositivo

En un sistema ESXi en ejecución, puede ver información sobre los alias de los adaptadores de E/S mediante la ejecución de comandos en un ESXi Shell.

Usar los comandos de ESXi Shell para ver la información de alias de un dispositivo

Comando	Descripción
`device alias list`	Enumera todos los alias de adaptadores de E/S actuales.
`device alias get -n<alias>`	Muestra el dispositivo físico al que se asigna un alias de adaptador de E/S.
`network nic list`	Enumera los alias e información general sobre los dispositivos de red.
`storage core adapter list`	Enumera todos los adaptadores de E/S de almacenamiento.

Nota Los comandos ESXCLI son compatibles. No se recomienda el uso de fuentes alternativas para mostrar información de alias.

Cambiar los alias de los dispositivos en un host ESXi mediante perfiles de host

El alias de un dispositivo en un host ESXi se puede modificar mediante la edición de la sección del alias de dispositivo del perfil del host asociado a los hosts.

La modificación de un alias de dispositivo se puede realizar, por ejemplo, cuando se aplica una actualización de BIOS o de firmware del dispositivo. Para obtener más información sobre los cambios en la configuración del alias de dispositivo, consulte Configuración de alias de dispositivo..

Los adaptadores de E/S que se basan en hardware PCI suelen tener una entrada de alias PCI y lógico. Ambos alias deben tener el mismo valor. Algunos adaptadores de E/S suelen tener solo una entrada de alias lógico. Los dispositivos de hardware PCI sin adaptadores de E/S suelen tener solo una entrada de alias PCI. Modifique una entrada de alias PCI solo cuando necesite el alias para otro dispositivo.

Nota Dos adaptadores de E/S diferentes no deben tener el mismo alias, excepto en el caso de adaptadores de E/S que se basen en el hardware PCI y tengan una entrada de alias lógico y PCI.

Procedimiento

Para obtener información sobre cómo exportar, extraer y editar un perfil de host, consulte el documento *Perfiles de host de vSphere*.

1 Exporte el perfil de host actual asociado al host ESXi.

2 Extraiga un nuevo perfil de host desde el host ESXi, pero no aplique el perfil del host.

3 Elimine todas las entradas de la sección de alias del dispositivo del perfil de host actual.

4 Transfiera todas las entradas desde la sección de alias del dispositivo del nuevo perfil de host a la misma sección del perfil de host actual.

   Puede modificar los alias de las entradas antes de agregarlas al perfil de host actual.

5 Vuelva a aplicar el perfil de host actual al host ESXi.

Cambiar los alias de los dispositivos en un host ESXi con estado mediante comandos ESXCLI

El alias de un dispositivo en un host ESXi con estado que no tenga un perfil de host asociado se puede modificar mediante la ejecución de comandos ESXCLI en el host.

La modificación de un alias de dispositivo se puede realizar, por ejemplo, cuando cambia la posición de ranura de un dispositivo. Para obtener más información sobre los cambios en la configuración del alias de dispositivo, consulte Configuración de alias de dispositivo..

Nota Es posible que los siguientes comandos ESXCLI no sean compatibles con la versión 6.7 de ESXi y otras versiones anteriores.

Procedimiento

1 Para ver una lista de la asignación actual de alias a las direcciones de dispositivos, en el ESXi Shell, ejecute `localcli --plugin-dir /usr/lib/vmware/esxcli/int/deviceInternal alias list`.

   En el caso de adaptadores de E/S que se basan en el hardware PCI, se suele ver una entrada de alias lógico y PCI.

   Para algunos adaptadores de E/S, se suele ver solo una entrada de alias lógico.

   En el caso de dispositivos de hardware PCI sin adaptadores de E/S, normalmente solo se ve una entrada de alias PCI.

2 Para modificar un alias, reemplace los valores de los marcadores de posición `ALIAS`, `PCI_ADDRESS` y `LOGICAL_ADDRESS` con valores reales y siga uno de los subpasos.

   a Si un adaptador de E/S tiene un alias PCI y otro lógico, ejecute `localcli --plugin-dir /usr/lib/vmware/esxcli/int/ deviceInternal alias store --bus-type logical --alias ALIAS --bus-address LOGICAL_ADDRESS` y `localcli --plugin-dir /usr/lib/vmware/esxcli/int/ deviceInternal alias store --bus-type pci --alias ALIAS --bus-address PCI_ADDRESS`.

      Los alias PCI y lógicos deben tener el mismo valor.

   b Si un adaptador de E/S solo tiene una entrada de alias lógico, ejecute `localcli --plugin-dir /usr/lib/vmware/esxcli/int/ deviceInternal alias store --bus-type logical --alias ALIAS --bus-address LOGICAL_ADDRESS`.

   c Si un dispositivo de hardware PCI solo tiene una entrada de alias PCI, ejecute `localcli --plugin-dir /usr/lib/vmware/esxcli/int/ deviceInternal alias store --bus-type pci --alias ALIAS --bus-address PCI_ADDRESS`.

      Modifique un alias PCI solo cuando necesite el alias para otro dispositivo.

   Nota Dos adaptadores de E/S diferentes no deben tener el mismo alias, excepto en el caso de adaptadores de E/S que se basen en el hardware PCI y tengan una entrada de alias lógico y PCI.

3 Reinicie el sistema.

Escenario de vSphere PowerCLI para vSphere Auto Deploy

Escenario para configurar un entorno de vSphere Auto Deploy en funcionamiento mediante PowerCLI.

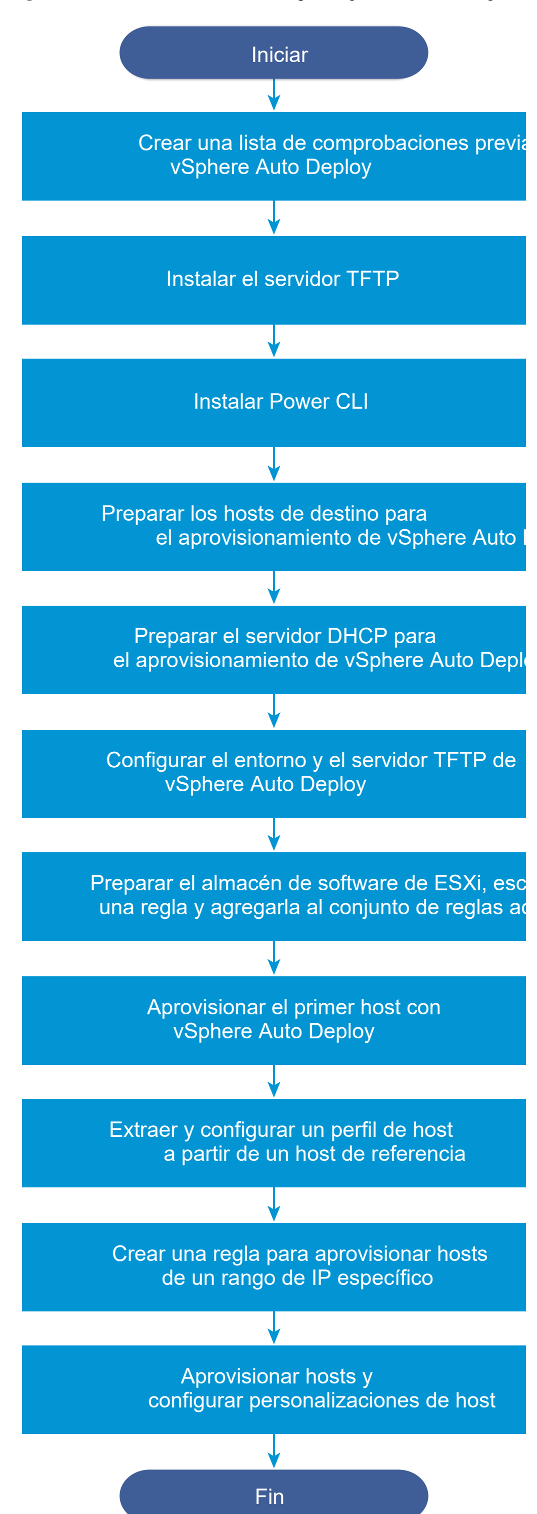
En este escenario, se va a configurar un entorno de trabajo de vSphere Auto Deploy que incluya cuatro hosts. Creará reglas y aprovisionará dos de los hosts con un perfil de imagen, y aprovisionará a los dos hosts restantes con el mismo perfil de imagen y un perfil de host configurado para solicitar la entrada del usuario. Este escenario le puede proporcionar la base para un entorno de producción. En las descripciones de las tareas se asume que va a utilizar una red común sin etiquetado de VLAN entre los hosts físicos y el resto de su entorno.

Para realizar las tareas de este escenario, deberá contar con los siguientes conocimientos y privilegios.

- Experiencia con vSphere (vCenter Server y ESXi).
- Conocimientos básicos sobre Microsoft PowerShell y PowerCLI.
- Derechos de administrador en un sistema Windows y un sistema de vCenter Server.

Siga las tareas en el orden presentado en este escenario. Algunos pasos pueden realizarse en un orden diferente, pero el orden utilizado aquí limita las manipulaciones repetidas de algunos componentes. Para obtener más información sobre la lista de comprobación previa a la instalación y otros requisitos previos para configurar vSphere Auto Deploy, consulte Instalar y configurar vSphere Auto Deploy.

Figura 4-11. Instalación y flujo de trabajo de aprovisionamiento de hosts de vSphere Auto Deploy



vSphere Auto Deploy aprovecha la infraestructura de iPXE; el arranque PXE con el firmware de BIOS heredado solo es posible en IPv4. Si los hosts que quiere aprovisionar con vSphere Auto Deploy presentan un BIOS heredado, el servidor vSphere Auto Deploy debe tener una dirección IPv4. El arranque PXE con firmware UEFI se puede realizar mediante IPv4 o IPv6.

Procedimiento

1 Instalar el servidor TFTP

Para configurar una infraestructura de vSphere Auto Deploy, es necesario instalar un servidor TFTP en el entorno. vSphere Auto Deploy depende de un servidor TFTP para enviar una imagen de arranque a los hosts que aprovisiona.

2 Instalar PowerCLI

Para poder administrar vSphere Auto Deploy mediante reglas creadas con cmdlets de PowerCLI, primero es necesario instalar PowerCLI.

3 Preparar los hosts de destino de vSphere Auto Deploy

Es necesario configurar los parámetros del BIOS para los cuatro hosts y volver a confirmar la dirección MAC del dispositivo de red principal a fin de preparar los hosts de destino para el aprovisionamiento con vSphere Auto Deploy.

4 Preparar el servidor DHCP para el aprovisionamiento de vSphere Auto Deploy

Cuando se preparan los hosts de destino de vSphere Auto Deploy, es necesario configurar el servidor DHCP de este escenario para proporcionar un archivo binario iPXE a cada host de destino.

5 Configure vSphere Auto Deploy y el entorno de TFTP en vSphere Client

Después de preparar el servidor DHCP, debe iniciar el servicio vSphere Auto Deploy vCenter Server y configurar el servidor TFTP. Debe descargar un archivo ZIP de TFTP del servidor vSphere Auto Deploy. El servidor FTP personalizado aloja las imágenes de arranque que proporciona vSphere Auto Deploy.

6 Preparar el almacén de software de ESXi y escribir una regla

Después de configurar la infraestructura de vSphere Auto Deploy, es necesario agregar un almacén de software de ESXi, especificar un perfil de imagen, escribir una regla y agregarla al conjunto de reglas activo.

7 Aprovisionar el primer host con vSphere Auto Deploy

Después de crear una regla y agregarla al conjunto de reglas activo, es posible aprovisionar el primer host y comprobar la ubicación de su vCenter Server para completar la verificación de aprovisionamiento de imagen de la instalación.

8 Extraer y configurar un perfil de host a partir de un host de referencia

Después de aprovisionar el primer host, es posible extraer y configurar un perfil de host que se puede usar para aplicar la misma configuración a otros hosts de destino. La configuración que varía en los distintos hosts, como la dirección IP estática, se puede administrar a través del mecanismo de personalización de host.

9 Crear una regla para aprovisionar hosts de un rango de IP específico

Después de crear un perfil de host a partir de un host de referencia, puede crear una regla para aplicar el perfil de imagen previamente verificado y el perfil de host extraído a hosts de destino en un rango de IP específico.

10 Aprovisionar hosts y configurar personalizaciones de host

Con la aplicación de la regla para aprovisionar hosts mediante un perfil de imagen y un perfil de host, es posible aprovisionar hosts de destino específicos. Si algún elemento del perfil de host está configurado para solicitar la intervención del usuario, el host se activa en modo de mantenimiento. Debe aplicar el perfil de host o comprobar el cumplimiento de host para que se le pida la información. El sistema asocia la personalización del host con el host.

Instalar el servidor TFTP

Para configurar una infraestructura de vSphere Auto Deploy, es necesario instalar un servidor TFTP en el entorno. vSphere Auto Deploy depende de un servidor TFTP para enviar una imagen de arranque a los hosts que aprovisiona.

Con esta tarea solo se instala el servidor TFTP. Después se descarga un archivo de configuración en el servidor. Consulte Configure vSphere Auto Deploy y el entorno de TFTP en vSphere Client.

Procedimiento

1. Descargue el servidor TFTP que prefiera en una ubicación que tenga acceso de red a su vCenter Server e instale el servidor.
2. Configure el directorio raíz TFTP, por ejemplo, `D:\TFTP_Root\`.

Pasos siguientes

Instale PowerCLI para administrar vSphere Auto Deploy con cmdlets de PowerCLI.

Instalar PowerCLI

Para poder administrar vSphere Auto Deploy mediante reglas creadas con cmdlets de PowerCLI, primero es necesario instalar PowerCLI.

Procedimiento

- Utilice la Guía del usuario de VMware PowerCLI para obtener información sobre los conceptos básicos de PowerShell, los conceptos de PowerCLI, y cómo instalar y configurar PowerCLI.

Pasos siguientes

Configure los parámetros de los hosts de destino con el fin de prepararlos para el aprovisionamiento con vSphere Auto Deploy.

Preparar los hosts de destino de vSphere Auto Deploy

Es necesario configurar los parámetros del BIOS para los cuatro hosts y volver a confirmar la dirección MAC del dispositivo de red principal a fin de preparar los hosts de destino para el aprovisionamiento con vSphere Auto Deploy.

Requisitos previos

Los hosts que se deseen aprovisionar con vSphere Auto Deploy deben cumplir con los requisitos para ESXi.

Consulte Requisitos de hardware de ESXi.

Procedimiento

1 Modifique la configuración del BIOS de cada uno de los cuatro hosts físicos para forzar el arranque de los hosts desde el dispositivo de red principal.

2 Vuelva a confirmar la dirección MAC del dispositivo de red principal.

Pasos siguientes

Configure el servidor DHCP para proporcionar a cada host de destino un archivo binario iPXE.

Preparar el servidor DHCP para el aprovisionamiento de vSphere Auto Deploy

Cuando se preparan los hosts de destino de vSphere Auto Deploy, es necesario configurar el servidor DHCP de este escenario para proporcionar un archivo binario iPXE a cada host de destino.

En el entorno de este escenario, se utiliza Active Directory con DNS y DHCP. El servidor DHCP se incluye en las versiones de vSphere compatibles con Windows Server.

Procedimiento

1 Inicie sesión en el servidor DHCP con privilegios de administrador.

2 Cree un ámbito DHCP para el intervalo de direcciones IP.

   a Haga clic en **Inicio > Configuración > Panel de control > Herramientas administrativas** y seleccione **DHCP**.

   b Desplácese hasta **DHCP >** ***hostname*** **> IPv4**.

   c Haga clic con el botón derecho en **IPv4** y seleccione **Nuevo ámbito**.

   d En la pantalla principal, haga clic en **Siguiente** y especifique un nombre y una descripción para el ámbito.

   e Especifique un intervalo de direcciones IP y haga clic en **Siguiente**.

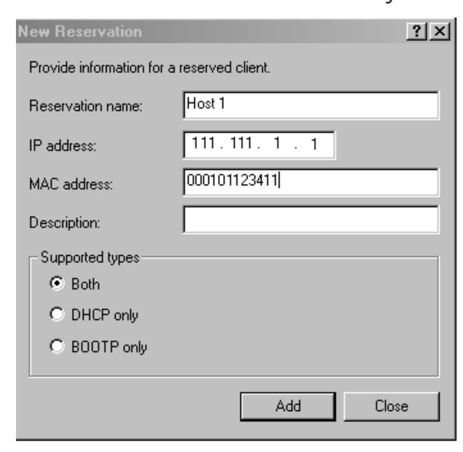
   f Haga clic en **Siguiente** hasta llegar a la pantalla Configurar opciones DHCP. Allí, seleccione **No, configuraré esta opción más adelante**.

3 Cree una reserva de DHCP para cada host ESXi de destino.

   a En la ventana DHCP, vaya a **DHCP** > ***hostname*** > **IPv4** > **Ámbito Auto Deploy** > **Reservas**.

   b Haga clic con el botón derecho en **Reservas** y seleccione **Nueva reserva**.

   c En la ventana Nueva reserva, especifique un nombre, una dirección IP y la dirección MAC de uno de los hosts. No incluya los dos puntos (:) en la dirección MAC.



   d Repita el procedimiento para cada uno de los otros hosts.

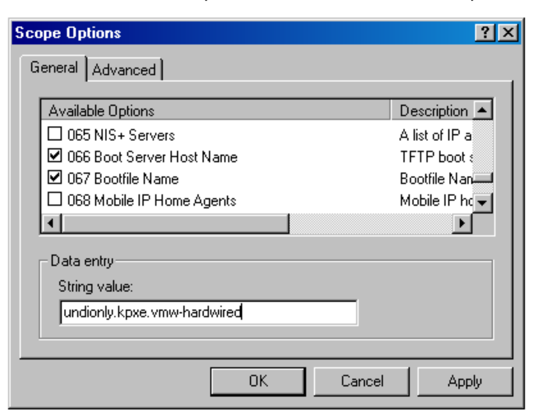
4 Configure el servidor DHCP para que apunte los hosts al servidor TFTP.

   a En la ventana DHCP, vaya a **DHCP** > ***hostname*** > **IPv4** > **Ámbito Auto Deploy** > **Opciones de ámbito**.

   b Haga clic con el botón derecho en **Opciones de ámbito** y elija **Configurar opciones**.

   c En la ventana Opciones de ámbito, haga clic en la pestaña **General**.

   d Haga clic en **066 Nombre de host de servidor de arranque** y escriba la dirección del servidor TFTP que instaló, en el campo Valor de cadena, debajo de Opciones disponibles.



e Haga clic en **067 Nombre de archivo de arranque** y escriba **`undionly.kpxe.vmw-hardwired`**.

El archivo binario iPXE `undionly.kpxe.vmw-hardwired` se utilizará para arrancar los hosts ESXi.

f Haga clic en **Aplicar** y, a continuación, en **Aceptar** para cerrar la ventana.

5 En la ventana DHCP, haga clic con el botón derecho en **DHCP > *hostname* > IPv4 > Ámbito > Activar** y haga clic en **Activar**.

6 Si va a utilizar Active Directory para DHCP y DNS, no cierre la sesión del servidor DHCP. De lo contrario, cierre sesión.

Pasos siguientes

Inicie el servicio vCenter Server de vSphere Auto Deploy y configure el servidor TFTP.

Configure vSphere Auto Deploy y el entorno de TFTP en vSphere Client

Después de preparar el servidor DHCP, debe iniciar el servicio vSphere Auto Deploy vCenter Server y configurar el servidor TFTP. Debe descargar un archivo ZIP de TFTP del servidor vSphere Auto Deploy. El servidor FTP personalizado aloja las imágenes de arranque que proporciona vSphere Auto Deploy.

Procedimiento

1 Utilice vSphere Client para conectarse al sistema vCenter Server que administra el servidor vSphere Auto Deploy.

2 Inicie el servicio vSphere Auto Deploy.

a Desplácese hasta **Inicio > Auto Deploy**.

b En la página **Auto Deploy**, seleccione la instancia de vCenter Server en el menú desplegable en la parte superior.

c Haga clic en **Habilitar Auto Deploy e Image Builder** para activar el servicio.

Si el servicio de **Image Builder** ya está activo, seleccione la pestaña **Configurar** y haga clic en **Habilitar servicio de Auto Deploy**.

3 En el inventario de Auto Deploy, haga clic en la pestaña **Configurar**.

4 Haga clic en **Descargar archivo zip de TFTP**.

5 Guarde el archivo`deploy-tftp.zip` en el directorio `TFTP_Root` que creó al instalar el servidor TFTP y descomprima el archivo.

Pasos siguientes

Agregue un almacén de software al inventario y utilice un perfil de imagen del almacén para crear una regla de aprovisionamiento de hosts.

Preparar el almacén de software de ESXi y escribir una regla

Después de configurar la infraestructura de vSphere Auto Deploy, es necesario agregar un almacén de software de ESXi, especificar un perfil de imagen, escribir una regla y agregarla al conjunto de reglas activo.

vSphere Auto Deploy aprovisiona hosts con perfiles de imagen donde se define el conjunto de VIB que se utiliza en un proceso de instalación de ESXi. Los perfiles de imágenes se almacenan en almacenes de software. Debe asegurarse de que esté disponible el perfil de imagen correcto antes de iniciar el aprovisionamiento de los hosts. Cuando se agrega un almacén de software a una sesión de PowerCLI, el almacén solo se encuentra disponible durante la sesión actual. No se mantiene de una sesión a otra.

Los pasos de esta tarea indican que se deben ejecutar cmdlets de PowerCLI. Para obtener información adicional sobre los cmdlets de vSphere Auto Deploy que se pueden ejecutar en una sesión de PowerCLI, consulte Descripción general de cmdlets de vSphere Auto Deploy PowerCLI.

Requisitos previos

Compruebe si puede acceder a los hosts ESXi que desea aprovisionar desde el sistema en el que se ejecuta PowerCLI.

Procedimiento

1 Inicie sesión como administrador en la consola del sistema Windows, ya sea de forma directa o mediante RDP.

   En esta tarea, se supone que PowerCLI se instaló en el sistema donde se ejecuta vCenter Server.

2 En una sesión de PowerCLI, ejecute el cmdlet `Connect-VIServer` para conectarse al sistema vCenter Server con el que se registró vSphere Auto Deploy.

   ```
   Connect-VIServer ipv4_address
   ```

   Es posible que el cmdlet devuelva una advertencia de certificado de servidor. En un entorno de producción, asegúrese de que no se produzca ningún problema de certificado de servidor. En un entorno de desarrollo, puede omitir la advertencia.

3 Introduzca las credenciales para vCenter Server.

4 Ejecute `Add-EsxSoftwareDepot` para agregar el almacén en línea a la sesión de PowerCLI.

   ```
   Add-EsxSoftwareDepot https://hostupdate.vmware.com/software/VUM/PRODUCTION/main/vmw-depot-index.xml
   ```

   Se requiere agregar el almacén de software cada vez que se inicia una sesión nueva de PowerCLI.

5 Revise el contenido del almacén de software con el cmdlet `Get-EsxImageProfile` para comprobar si se agregó correctamente el almacén.

   El cmdlet devuelve información sobre todos los perfiles de imágenes en el almacén.

6 Ejecute el cmdlet `New-DeployRule` para crear una nueva regla.

```
New-DeployRule -Name "InitialBootRule" -Item ESXi-6.0.0-2494585-standard -AllHosts
```

El cmdlet creará una regla para asignar el perfil de imagen especificado a todos los hosts del inventario.

7 Agregue la nueva regla al conjunto de reglas activo con la finalidad de que la regla esté disponible para el servidor vSphere Auto Deploy.

```
Add-DeployRule    -DeployRule "InitialBootRule"
```

Pasos siguientes

Aprovisione el primer host con vSphere Auto Deploy y revise su aprovisionamiento de imagen.

Aprovisionar el primer host con vSphere Auto Deploy

Después de crear una regla y agregarla al conjunto de reglas activo, es posible aprovisionar el primer host y comprobar la ubicación de su vCenter Server para completar la verificación de aprovisionamiento de imagen de la instalación.

Procedimiento

1 Abra una sesión de consola en el host físico que desee utilizar como el primer host ESXi de destino, arranque el host y busque mensajes que indiquen un arranque iPXE correcto.

   Durante el proceso de arranque, DHCP asigna una dirección IP al host. La dirección IP coincide con el nombre que especificó anteriormente en el servidor DNS. El host se pone en contacto con el servidor vSphere Auto Deploy y descarga los archivos binarios de ESXi desde la dirección URL de HTTP indicada en el archivo tramp de iPXE que descargó anteriormente al directorio TFTP_Root. Cada instancia de vSphere Auto Deploy produce un conjunto de archivos personalizado para el servidor TFTP.

2 Utilice vSphere Client para conectarse al sistema vCenter Server que administra el servidor vSphere Auto Deploy.

3 En la página de inicio de vSphere Client, haga clic en **Hosts y clústeres**.

4 Compruebe que el host recientemente aprovisionado se encuentre ahora en el inventario de vCenter Server en el nivel del centro de datos.

   De forma predeterminada, vSphere Auto Deploy agrega hosts en ese nivel cuando se completa el proceso de arranque.

Pasos siguientes

Extraiga un perfil de host del host y configúrelo para se requieran entradas del usuario.

Extraer y configurar un perfil de host a partir de un host de referencia

Después de aprovisionar el primer host, es posible extraer y configurar un perfil de host que se puede usar para aplicar la misma configuración a otros hosts de destino. La configuración

que varía en los distintos hosts, como la dirección IP estática, se puede administrar a través del mecanismo de personalización de host.

vSphere Auto Deploy puede aprovisionar todos los hosts con el mismo perfil de host. vSphere Auto Deploy también puede utilizar la personalización de host para especificar información diferente para diversos hosts. Por ejemplo, si configura un puerto VMkernel para vMotion o para almacenamiento, puede especificar una dirección IP estática para el puerto mediante el mecanismo de personalización de host.

Procedimiento

1 Utilice vSphere Client para conectarse al sistema vCenter Server que administra el servidor vSphere Auto Deploy.

2 Haga clic en **Directivas y perfiles** y seleccione **Perfiles de host**.

3 Haga clic en **Extraer perfil de host**.

4 En la página **Seleccionar host** del asistente, seleccione el host de referencia que configuró antes y haga clic en **Siguiente**.

5 En la página **Nombre y descripción** del asistente, introduzca un nombre y una descripción para el nuevo perfil y haga clic en **Finalizar**.

6 Seleccione el perfil de host que desea editar y haga clic en la pestaña **Configurar**.

7 Haga clic en **Editar perfil de host**.

8 Seleccione **Seguridad y servicios > Configuración de seguridad > Seguridad > Configuración de usuario > raíz**.

9 En el menú desplegable **Contraseña**, seleccione **Configuración de contraseña introducida por el usuario**.

10 Haga clic en **Guardar** para configurar los ajustes del perfil de host.

Pasos siguientes

Cree una regla de vSphere Auto Deploy para aplicar el perfil de host a otros hosts ESXi.

Crear una regla para aprovisionar hosts de un rango de IP específico

Después de crear un perfil de host a partir de un host de referencia, puede crear una regla para aplicar el perfil de imagen previamente verificado y el perfil de host extraído a hosts de destino en un rango de IP específico.

Procedimiento

1 Inicie sesión con privilegios de administrador en la consola del sistema Windows, ya sea de forma directa o mediante RDP.

2 En una sesión de PowerCLI, ejecute el cmdlet `Connect-VIServer` para conectarse al sistema vCenter Server con el que se registró vSphere Auto Deploy.

```
Connect-VIServer ipv4_address
```

Es posible que el cmdlet devuelva una advertencia de certificado de servidor. En un entorno de producción, asegúrese de que no se produzca ningún problema de certificado de servidor. En un entorno de desarrollo, puede omitir la advertencia.

3 Ejecute `Add-EsxSoftwareDepot` para agregar el almacén en línea a la sesión de PowerCLI.

```
Add-EsxSoftwareDepot https://hostupdate.vmware.com/software/VUM/PRODUCTION/main/vmw-depot-
index.xml
```

Se requiere agregar el almacén de software cada vez que se inicia una sesión nueva de PowerCLI.

4 (Requerido) Ejecute el cmdlet `Get-DeployRuleset` para ver las reglas en el conjunto de reglas activo.

5 Cree una regla para indicar a vSphere Auto Deploy que debe aprovisionar el conjunto de hosts de un rango de IP específico con el perfil de imagen anteriormente seleccionado y el perfil de host creado a partir del host de referencia.

```
New-DeployRule -name "Production01Rule" -item "image_profile",ESXiGold -Pattern
"ipv4=IP_range"
```

6 Agregue la nueva regla al conjunto de reglas activo.

```
Add-DeployRule    -DeployRule "Production01Rule"
```

7 Ejecute el comando `Get-DeployRuleset` para comprobar el conjunto de reglas activo.

En PowerCLI, se muestra información similar a la del siguiente ejemplo.

```
Name:              Production01Rule
PatternList:       {ipv4=address_range}
ItemList:          {ESXi-version-XXXXXX-standard, Compute01, ESXiGold}
```

Pasos siguientes

Aprovisione los hosts y configure personalizaciones de host.

Aprovisionar hosts y configurar personalizaciones de host

Con la aplicación de la regla para aprovisionar hosts mediante un perfil de imagen y un perfil de host, es posible aprovisionar hosts de destino específicos. Si algún elemento del perfil de host está configurado para solicitar la intervención del usuario, el host se activa en modo de mantenimiento. Debe aplicar el perfil de host o comprobar el cumplimiento de host para que se le pida la información. El sistema asocia la personalización del host con el host.

Procedimiento

1 Arranque el resto de los hosts que desea aprovisionar.

   vSphere Auto Deploy arranca los hosts, aplica el perfil de host y agrega los hosts al inventario de vCenter Server. Los hosts permanecen en el modo de mantenimiento, dado que el perfil de host de referencia está configurado para solicitar la intervención del usuario para cada host.

2 Utilice vSphere Client para conectarse al sistema vCenter Server que administra el servidor vSphere Auto Deploy.

3 Haga clic en **Directivas y perfiles** y seleccione **Perfiles de host**.

4 Haga clic con el botón secundario en el perfil de host recién creado para Auto Deploy y luego en **Editar personalizaciones de host**.

5 Seleccione los hosts, introduzca las personalizaciones de host requeridas y haga clic en **Finalizar**.

   Si lo prefiere, también puede **Importar personalizaciones de host**.

6 Aplique el perfil de host a cada uno de los hosts y desactive el modo de mantenimiento de los hosts. Como alternativa, puede reiniciar cada host.

   Una vez finalizado el progreso de reinicio, todo los hosts están en ejecución con la imagen que especifica y utiliza la configuración del perfil de host de referencia. El clúster muestra que todos los hosts son totalmente compatibles.

Resultados

Ahora todos los hosts están configurados con información compartida a través del perfil de host de referencia y con la información específica del host a través del mecanismo de personalización de host. En el próximo arranque, los hosts recibirán toda la información de perfil de host, incluidos los datos específicos de cada host, y se iniciarán totalmente configurados y fuera del modo de mantenimiento.

Solución de problemas de vSphere Auto Deploy

Los temas de solución de problemas de vSphere Auto Deploy cubren situaciones en las que el aprovisionamiento de hosts con vSphere Auto Deploy no funciona según lo esperado.

La regla de vSphere Auto Deploy tarda mucho en completarse

Después de ejecutar una regla de Auto Deploy, tarda mucho en completarse y no se ve ningún progreso para las tareas.

Problema

Auto Deploy detecta automáticamente si hay disponible una nueva versión de la imagen que utiliza un clúster, o cuando caduca la duración de la memoria caché de los archivos, y actualiza la memoria caché volviendo a descargar los archivos de la versión más reciente del almacén de software. Como resultado, es posible que se produzca un retraso en la implementación de las reglas de Auto Deploy.

Causa

Cuando caduca la duración de la memoria caché de los archivos almacenados en caché por Auto Deploy, Auto Deploy actualiza automáticamente la memoria caché desde el almacén de software. Debido a que un almacén de software predeterminado suele ser de más de 300 MB, dependiendo de la red, la descarga puede tardar mucho tiempo.

También puede observar un retraso en la implementación de las reglas de Auto Deploy al convertir un clúster que se administra con una sola imagen en uno que se administra con una configuración en un nivel de clúster. Si un host intenta arrancar durante el tiempo que Auto Deploy almacena en caché el archivo de configuración, es posible que se produzca un retraso debido al tiempo que Auto Deploy necesita para crear la memoria caché.

Un problema general de infraestructura de vSphere también puede impedir que las reglas de Auto Deploy se ejecuten correctamente.

Solución

- Independientemente de si hay problemas de conectividad o interrupciones, Auto Deploy mantiene las sesiones activas y persiste en el arranque de los hosts hasta que tiene éxito.

Error de tiempo de espera de TFTP de vSphere Auto Deploy durante el arranque

Se muestra el mensaje de error de tiempo de espera de TFTP en el arranque de un host aprovisionado con vSphere Auto Deploy. El texto del mensaje depende del BIOS.

Problema

Se muestra el mensaje de error de tiempo de espera de TFTP en el arranque de un host aprovisionado con vSphere Auto Deploy. El texto del mensaje depende del BIOS.

Causa

El servidor TFTP está caído o no está accesible.

Solución

- Asegúrese de que el servicio TFTP esté en ejecución y accesible para el host que está intentando arrancar.
- Para ver los registros de diagnóstico y obtener más información sobre el error presente, consulte la documentación del servicio TFTP.

El host vSphere Auto Deploy arranca con una configuración incorrecta

Un host está arrancando con una imagen, perfil de host o ubicación de carpeta de ESXi diferentes de los especificados en las reglas.

Problema

Un host está arrancando con un perfil de imagen o configuración de ESXi diferentes a los que especifican las reglas. Por ejemplo, puede cambiar las reglas para asignar un perfil de imagen diferente, pero el host sigue usando el perfil de imagen antiguo.

Causa

Una vez que se agrega el host a un sistema vCenter Server, el sistema vCenter Server determina la configuración de arranque. El sistema vCenter Server asociará un perfil de imagen, un perfil de host o la ubicación de carpeta con el host.

Solución

- Use los cmdlets de vSphere PowerCLI `Test-DeployRuleSetCompliance` y `Repair-DeployRuleSetCompliance` para reevaluar las reglas y asociar el perfil de imagen, el perfil de host o la ubicación de carpeta correctos con el host.

No se redirige el host al servidor vSphere Auto Deploy

Durante un arranque, un host que se desea aprovisionar con vSphere Auto Deploy carga iPXE. El host no se redirige al servidor vSphere Auto Deploy.

Problema

Durante un arranque, un host que se desea aprovisionar con vSphere Auto Deploy carga iPXE. El host no se redirige al servidor vSphere Auto Deploy.

Causa

El archivo `tramp` que se incluye en el archivo ZIP TFTP tiene la dirección IP incorrecta para el servidor vSphere Auto Deploy.

Solución

- Corrija la dirección IP del servidor vSphere Auto Deploy en el archivo `tramp`, según se explica en la documentación *Instalación y configuración de vSphere*.

Mensaje de advertencia de paquete cuando se asigna un perfil de imagen al host vSphere Auto Deploy

Cuando se ejecuta un cmdlet de vSphere PowerCLI para asignar un perfil de imagen que no está preparado para vSphere Auto Deploy, se muestra un mensaje de advertencia.

Problema

Cuando escribe o modifica reglas para asignar un perfil de imagen a uno o más hosts, se produce el siguiente error:

```
Warning: Image Profile <name-here> contains one or more software packages
that are not stateless-ready. You may experience problems when using this
profile with Auto Deploy.
```

Causa

Cada VIB en un perfil de imagen tiene una marca `stateless-ready` para indicar que el VIB se diseñó para usarse con vSphere Auto Deploy. El error se produce al intentar escribir una regla de vSphere Auto Deploy donde se usa un perfil de imagen en el cual uno o más VIB tienen esa marca establecida en FALSE.

Nota Es posible usar sin problemas los hosts aprovisionados con vSphere Auto Deploy que incluyen VIB no preparados para estar sin estado. Sin embargo, un arranque con un perfil de imagen que incluye VIB que no están preparados para estar sin estado se trata como una instalación nueva. Cada vez que se arranca el host, se pierden datos de configuración que se encontrarían disponibles a través de reinicios para hosts aprovisionados con vSphere Auto Deploy.

Solución

1. Utilice cmdlets de vSphere ESXi Image Builder en una sesión de vSphere PowerCLI para ver los VIB en el perfil de imagen.
2. Quite cualquier VIB que no esté preparado para estar sin estado.
3. Vuelva a ejecutar el cmdlet de vSphere Auto Deploy.

El host vSphere Auto Deploy con una unidad flash USB integrada no envía volcados de memoria al disco local

Si el host vSphere Auto Deploy presenta una unidad flash USB integrada y un error produce un volcado de memoria, el volcado se pierde. Configure el sistema de modo que se use ESXi Dump Collector para almacenar volcados de memoria en un host en red.

Problema

Si el host vSphere Auto Deploy presenta una unidad USB flash integrada y se detecta que un error produce un volcado de memoria, el volcado de memoria no se envía al disco local.

Solución

1. Instale ESXi Dump Collector en el sistema de su elección.

   ESXi Dump Collector se incluye con el instalador de vCenter Server.
2. Use ESXCLI para configurar el host de modo que use ESXi Dump Collector.

   ```
   esxcli conn_options system coredump network set IP-addr,port
   esxcli system coredump network set -e true
   ```

3 Utilice ESXCLI para desactivar las particiones de volcado de núcleo locales.

```
esxcli conn_options system coredump partition set -e false
```

El host vSphere Auto Deploy se reinicia después de cinco minutos

El host vSphere Auto Deploy arranca y muestra información de iPXE, pero se reinicia tras cinco minutos.

Problema

Un host que se aprovisionará con vSphere Auto Deploy arranca desde iPXE y muestra información de iPXE en la consola. Sin embargo, tras cinco minutos, el host muestra el siguiente mensaje a la consola y se reinicia.

```
This host is attempting to network-boot using VMware
AutoDeploy. However, there is no ESXi image associated with this host.
Details: No rules containing an Image Profile match this
host. You can create a rule with the New-DeployRule PowerCLI cmdlet
and add it to the rule set with Add-DeployRule or Set-DeployRuleSet.
The rule should have a pattern that matches one or more of the attributes
listed below.
```

El host también podría mostrar los siguientes detalles:

```
Details: This host has been added to VC, but no Image Profile
is associated with it. You can use Apply-ESXImageProfile in the
PowerCLI to associate an Image Profile with this host.
Alternatively, you can reevaluate the rules for this host with the
Test-DeployRuleSetCompliance and Repair-DeployRuleSetCompliance cmdlets.
```

Luego, la consola muestra los atributos de las máquinas del host incluido el proveedor, el número de serie, la dirección IP, etc.

Causa

No hay un perfil de imagen actualmente asociado con este host.

Solución

Es posible asignar un perfil de imagen al host. Para ello, ejecute el cmdlet `Apply-EsxImageProfile` o cree la siguiente regla:

1 Ejecute el cmdlet `New-DeployRule` para crear una regla que incluya un patrón que coincida con el host con un perfil de imagen.

2 Ejecute el cmdlet `Add-DeployRule` para agregar la regla a un conjunto de reglas.

3 Ejecute el cmdlet `Test-DeployRuleSetCompliance` y use el resultado de ese cmdlet como entrada para el cmdlet de `Repair-DeployRuleSetCompliance`.

El host vSphere Auto Deploy no puede contactar con el servidor TFTP

El host que se aprovisiona con vSphere Auto Deploy no puede contactar con el servidor TFTP.

Problema

Cuando se intenta arrancar un host aprovisionado con vSphere Auto Deploy, el host realiza un arranque de red y el servidor DHCP le asigna una dirección DHCP, pero el host no puede contactar con el servidor TFTP.

Causa

El servidor TFTP podría haber dejado de ejecutarse o un firewall podría bloquear el puerto TFTP.

Solución

- Si instaló el servidor TFTP de WinAgents, abra la consola de administración TFTP de TFTP y compruebe que el servicio esté en ejecución. Si el servicio se está ejecutando, compruebe las reglas de entrada del firewall de Windows para asegurarse de que el puerto TFTP no esté bloqueado. Desactive temporalmente el firewall para ver si este es el problema.
- Para todos los otros servidores TFTP, consulte la documentación para procedimientos de depuración.

El host vSphere Auto Deploy no puede recuperar una imagen de ESXi del servidor vSphere Auto Deploy

El host que se aprovisiona con vSphere Auto Deploy se detiene en la pantalla de arranque de iPXE.

Problema

Cuando se intenta arrancar un host aprovisionado con vSphere Auto Deploy, el proceso de arranque se detiene en la pantalla de arranque de iPXE y el mensaje de estado indica que el host intenta obtener la imagen de ESXi del servidor vSphere Auto Deploy.

Causa

Es posible que el servicio de vSphere Auto Deploy se haya detenido o que no se pueda acceder al servidor vSphere Auto Deploy.

Solución

1. Inicie sesión en el sistema en el cual instaló el servidor vSphere Auto Deploy.
2. Compruebe que el servidor vSphere Auto Deploy esté en ejecución.
   a. Haga clic en **Inicio** > **Configuración** > **Panel de control** > **Herramientas administrativas**.
   b. Haga doble clic en **Servicios** para abrir el panel Administración de servicios.
   c. En el campo Servicios, busque el servicio VMware vSphere Auto Deploy Waiter y reinícielo si no está en ejecución.

3 Abra un explorador web, introduzca la siguiente URL y compruebe si es posible acceder al servidor vSphere Auto Deploy.

https://*Auto_Deploy_Server_IP_Address*:*Auto_Deploy_Server_Port*/vmw/rdb

Nota Use esta dirección solo para comprobar si se puede tener acceso al servidor.

4 Si no es posible hacerlo, probablemente hay un problema con el firewall.

   a Intente configurar reglas de entrada de TCP permisivas para el puerto del servidor vSphere Auto Deploy.

   El puerto es 6501 a menos que haya especificado uno diferente durante la instalación.

   b Como último recurso, desactive temporalmente el firewall y vuelva a habilitarlo después de que haya verificado si bloqueó el tráfico. No desactive el firewall en entornos de producción.

   Para desactivar el firewall, ejecute **`netsh firewall set opmode disable`**. Para habilitar el firewall, ejecute **`netsh firewall set opmode enable`**.

El host vSphere Auto Deploy no obtiene una dirección asignada por DHCP

El host que se aprovisiona con vSphere Auto Deploy no recibe una dirección DHCP.

Problema

Cuanto se intenta arrancar un host aprovisionado con vSphere Auto Deploy, el host realiza un arranque de red, pero presenta una dirección DHCP asignada. El servidor vSphere Auto Deploy no puede aprovisionar el host con el perfil de imagen.

Causa

Puede que tenga un problema con el servicio DHCP o con la instalación del firewall.

Solución

1 Compruebe que el servicio de servidor DHCP esté ejecutándose en el sistema Windows en el cual el servidor DHCP está instalado para aprovisionar hosts.

   a Haga clic en **Inicio > Configuración > Panel de control > Herramientas administrativas**.

   b Haga doble clic en **Servicios** para abrir el panel Administración de servicios.

   c En el campo Servicios, busque el servicio de servidor DHCP y reinicie el servicio si no está en ejecución.

2 Si el servidor DHCP está en ejecución, vuelva a comprobar el ámbito de DHCP y las reservas de DHCP que configuró para sus hosts de destino.

   Si el ámbito y reservas de DHCP están configurados de forma correcta, lo más probable es que el problema involucre al firewall.

3 Como solución alternativa temporal, apague el firewall para ver si eso resuelve el problema.

   a Abra el símbolo del sistema haciendo clic en **Inicio > Programa > Accesorios > Símbolo del sistema**.

   b Escriba el siguiente comando para apagar temporalmente el firewall. No apague el firewall en un entorno de producción.

   ```
   netsh firewall set opmode disable
   ```

   c Intente aprovisionar el host con vSphere Auto Deploy.

   d Escriba el siguiente comando para volver a encender el firewall.

   ```
   netsh firewall set opmode enable
   ```

4 Instale reglas para permitir tráfico de red DHCP hacia los hosts de destino.

   Consulte la documentación del firewall para ver los detalles del DHCP y del sistema Windows en el cual se ejecuta el servidor DHCP.

El host vSphere Auto Deploy no realiza el arranque de red

El host que se aprovisiona con vSphere Auto Deploy se activa, pero no realiza el arranque de red.

Problema

Cuando se intenta arrancar un host aprovisionado con vSphere Auto Deploy, el host no inicia el proceso de arranque de red.

Causa

No habilitó el host para el arranque de red.

Solución

1 Reinicie el host y siga las instrucciones en pantalla para acceder a la configuración del BIOS.

2 En la configuración del BIOS, habilite el arranque de red en la configuración de dispositivo de arranque.

Recuperarse de daños en la base de datos en el servidor vSphere Auto Deploy

En ciertas situaciones, es posible que experimente un problema con la base de datos de vSphere Auto Deploy. La opción de recuperación más eficaz es reemplazar el archivo de base de datos actual con la copia de seguridad más reciente.

Problema

Al usar vSphere Auto Deploy para aprovisionar los hosts ESXi del entorno, es posible que experimente un problema con la base de datos de vSphere Auto Deploy.

Importante Se trata de un problema poco frecuente. Siga todas las demás estrategias de solución de problemas de vSphere Auto Deploy antes de reemplazar el archivo de base de datos actual. Se perderán las reglas o las asociaciones que haya creado desde la copia de seguridad que elija.

Causa

Este problema ocurre únicamente en los hosts aprovisionados con vSphere Auto Deploy.

Solución

1 Detenga el servicio del servidor vSphere Auto Deploy.

2 Busque el registro de vSphere Auto Deploy desde la página de vSphere Auto Deploy en vSphere Client.

3 Busque el siguiente mensaje en los registros:

   `DatabaseError: database disk image is malformed.`

   Si ve este mensaje, reemplace el archivo de base de datos existente con la copia de seguridad más reciente.

4 Vaya al directorio de datos de vSphere Auto Deploy en `/var/lib/rbd`.

   El directorio contiene un archivo denominado `db` y los archivos de copia de seguridad denominados `db`-*aaa-mm-dd*.

5 Cambie el nombre del archivo `db` actual.

   Si solicita asistencia, es posible que el servicio de soporte de VMware le pida ese archivo.

6 Cambie el nombre de la copia de seguridad más reciente a `db`.

7 Reinicie el servicio del servidor vSphere Auto Deploy.

8 Si el mensaje sigue apareciendo en el registro, repita los pasos para usar la siguiente copia de seguridad más reciente hasta que vSphere Auto Deploy funcione sin mostrar errores de la base de datos.

Configurar ESXi

Estos temas proporcionan información sobre el uso de la interfaz de usuario de la consola directa y la configuración de los valores predeterminados de ESXi.

Configuración inicial de ESXi

Configurar ESXi automáticamente

Cuando enciende el host ESXi por primera vez o después de restablecer los valores predeterminados de configuración, el host pasa a la fase de autoconfiguración. En esta fase se configuran dispositivos de red y de almacenamiento del sistema con opciones predeterminadas.

De manera predeterminada, el protocolo de configuración dinámica de host (DHCP) configura IP y todos los discos internos visibles que están en blanco se formatean con el sistema de archivos de la máquina virtual (VMFS). De este modo, las máquinas virtuales pueden almacenarse en los discos.

Qué leer a continuación

Administrar ESXi de forma remota

Puede utilizar VMware Host Client, vSphere Client y vCenter Server para administrar los hosts ESXi.

Para obtener instrucciones sobre cómo descargar e instalar vCenter Server y los componentes de vCenter Server, consulte *Instalar y configurar vCenter Server*. Para obtener información sobre cómo instalar VMware Host Client, consulte *Administración de hosts de vSphere Single*.

Acerca de la interfaz de ESXi de la consola directa

Use la consola directa para la configuración inicial y solución de problemas de ESXi.

Conecte un teclado y monitor al host para usar la consola directa. Una vez que el host concluye la fase de configuración automática, aparece la consola directa en el monitor. Puede examinar la configuración de red predeterminada y cambiar cualquier configuración que no sea compatible con el entorno de red.

Las operaciones clave disponibles en la consola directa incluyen:

- Configuración de hosts
- Configuración de acceso administrativo
- Solucionar problemas

También puede usar vSphere Client para administrar el host mediante vCenter Server.

Tabla 4-20. Buscar en la consola directa

Acción	Clave
Ver y cambiar la configuración	F2
Cambiar la interfaz de usuario a modo de alto contraste	F4
Apagar o reiniciar el host	F12
Ver el registro de VMkernel	Alt+F12
Cambiar a la consola del shell	Alt+F1

Tabla 4-20. Buscar en la consola directa (continuación)

Acción	Clave
Cambiar a la interfaz de usuario de la consola directa	Alt+F2
Mover la selección entre campos	Teclas de flecha
Seleccionar un elemento de menú	Intro
Alternar un valor	Barra espaciadora
Confirmar comandos sensibles, como restablecimiento de valores predeterminados de la configuración	F11
Guardar y salir	Intro
Salir sin guardar	Esc
Salir de registros del sistema	q

Configuración de la distribución del teclado para la consola directa

Puede configurar la distribución del teclado que desea usar con la consola directa.

Procedimiento

1 Desde la consola directa, seleccione **Configurar teclado** y presione Intro.

2 Seleccione la distribución que desea usar.

3 Presione la barra espaciadora para habilitar y desactivar las selecciones.

4 Presione Intro.

Crear un mensaje emergente de seguridad para la consola directa

Un banner de seguridad es un mensaje que se muestra en la pantalla **Principal** de la consola directa.

Procedimiento

1 Desde vSphere Client, conéctese a vCenter Server.

2 Seleccione el host en el inventario.

3 Haga clic en la pestaña **Configurar**.

4 En Sistema, seleccione **Configuración avanzada del sistema**.

5 Seleccione `Annotations.WelcomeMessage`.

6 Haga clic en el icono **Editar**.

7 Introduzca un mensaje de seguridad.

Resultados

El mensaje se muestra en la pantalla **Principal** de la consola directa.

Redirigir la consola directa a un puerto serie

Para administrar de forma remota el host ESXi desde una consola serie, puede redirigir la consola directa hacia un puerto serie.

vSphere admite el tipo de terminal VT100 y el emulador de terminal PuTTy para ver la consola directa a través del puerto serie.

Puede redirigir la consola directa hacia un puerto serie de varias formas.

Qué leer a continuación

Redireccionar la consola directa a un puerto serie mediante la configuración manual de las opciones de arranque

Cuando se redirige la consola directa a un puerto serie mediante la configuración de opciones de arranque, el cambio no persiste en los arranques subsiguientes.

Requisitos previos

Compruebe que el puerto serie no esté en uso para la generación de registros y la depuración serie.

Procedimiento

1. Inicie el host.
2. Cuando aparezca la ventana Cargando el hipervisor de VMware, presione las teclas Mayús + O para editar las opciones de arranque.
3. Desactive logPort y gdbPort en com1 y establezca tty2Port en com1 introduciendo las siguientes opciones de arranque:

   ```
   "gdbPort=none logPort=none tty2Port=com1";
   ```

   Para utilizar com2, reemplace `com1` por `com2`.

Resultados

La consola directa se redirecciona al puerto serie hasta que reinicie el host. Para redireccionar la consola directa para los arranque subsiguientes, consulte Redirigir la consola directa a un puerto serie desde vSphere Client

Redirigir la consola directa a un puerto serie desde vSphere Client

Puede administrar de forma remota el host ESXi desde una consola que esté conectada al puerto serie redirigiendo la consola directa a los puertos serie com1 o com2. Cuando se utiliza vSphere

Client para redirigir la consola directa a un puerto serie, la opción de arranque que se configura continúa después de los arranques posteriores.

Requisitos previos

- Compruebe que puede acceder al host desde vSphere Client.
- Compruebe que el puerto serie no esté en uso para registro y depuración seriales o para shell ESX (tty1Port).

Procedimiento

1 Desde vSphere Client, conéctese a vCenter Server.

2 Seleccione el host en el inventario.

3 Haga clic en la pestaña **Configurar**.

4 En Sistema, seleccione **Configuración avanzada del sistema**.

5 Asegúrese de que los campos **VMkernel.Boot.logPort** y **VMkernel.Boot.gdbPort** no estén establecidos para usar el puerto com al que desea redirigir la consola directa.

6 Configure **VMkernel.Boot.tty2Port** al puerto serie para redireccionar la consola directa a: **`com1`** o **`com2`**.

7 Reinicie el host.

Resultados

Ahora puede administrar de forma remota el host ESXi desde una consola que esté conectada al puerto serie.

Redireccionar la consola directa a un puerto serie en un host implementado con Auto Deploy

Después de redireccionar la consola directa a un puerto serie, puede determinar que esa configuración forme parte del perfil de host que se conserva cuando se reaprovisiona el host con Auto Deploy.

Requisitos previos

El puerto serie no deberá estar en uso para el registro y la depuración en serie.

Procedimiento

1 Desde , conéctese a vCenter Server.

2 Seleccione el host en el inventario.

3 En Sistema, seleccione **Configuración avanzada del sistema**.

4 Asegúrese de que los campos **VMkernel.Boot.logPort** y **VMkernel.Boot.gdbPort** no estén establecidos para usar el puerto com al que desea redirigir la consola directa.

5 Configure **VMkernel.Boot.tty2Port** al puerto serie para redireccionar la consola directa a: **`com1`** o **`com2`**.

6 Haga clic en **Aceptar**.

7 Guarde el perfil de host y conecte el host al perfil. Consulte la documentación de *Perfiles de host de vSphere*.

Resultados

La configuración para redireccionar la consola directa a un puerto serie es almacenada por vCenter Server y se conserva cuando se reaprovisiona el host con Auto Deploy.

Habilitar el acceso a ESXi Shell y SSH con la interfaz de usuario de la consola directa

Use la interfaz de usuario de la consola directa para habilitar ESXi Shell.

Procedimiento

1 En la interfaz de usuario de la consola directa, presione F2 para acceder al menú Personalización del sistema.

2 Seleccione **Opciones de solución de problemas** y presione Intro.

3 En el menú Opciones del modo de solución de problemas, seleccione un servicio para habilitar.

   - Habilitar ESXi Shell
   - Habilitar SSH

4 Presione Intro para habilitar el servicio.

5 (opcional) Establezca el tiempo de espera de ESXi Shell.

   De forma predeterminada, el tiempo de espera de ESXi Shell es 0 (no activado).

   La configuración del tiempo de espera de disponibilidad es la cantidad de minutos que pueden transcurrir antes de que deba iniciar sesión después de que se habilite ESXi Shell. Después del período de tiempo de espera, si no se ha iniciado sesión, el shell se desactiva.

   Nota Si inicia sesión y se agota el tiempo de espera, la sesión se mantiene activa. No obstante, se desactiva ESXi Shell, lo que impide que otros usuarios inicien sesión.

   a En el menú Opciones del modo de solución de problemas, seleccione **Modificar tiempos de espera de SSH y ESXi Shell** y presione Intro.

   b Introduzca el tiempo de espera de disponibilidad en minutos.

      El tiempo de espera de disponibilidad es la cantidad de minutos que pueden transcurrir antes de que deba iniciar sesión después de que se habilite ESXi Shell.

c Presione Intro.

d Introduzca el tiempo de espera de inactividad.

El tiempo de inactividad es la cantidad de minutos que pueden transcurrir antes de que el usuario cierre sesión en sesiones interactivas inactivas. Los cambios en el tiempo de espera de inactividad se aplican la próxima vez que un usuario inicia sesión en ESXi Shell y no afectan las sesiones actuales.

6 Presione Esc hasta que vuelva al menú principal de la interfaz de usuario de la consola directa.

Configurar la contraseña de la cuenta de administrador

Puede usar la consola directa para establecer la contraseña para la cuenta de administrador (raíz).

El nombre de usuario del administrador para el host ESXi es root. De forma predeterminada, la contraseña del administrador no está establecida.

Procedimiento

1 En la consola directa, seleccione **Configurar contraseña**.

2 (opcional) Si ya hay una contraseña configurada, escríbala en la línea **Contraseña antigua** y presione Intro.

3 En la línea **Contraseña nueva**, introduzca una nueva contraseña y presione Intro.

4 Vuelva a introducir la nueva contraseña y presione Intro.

Configuración de arranque del BIOS

Si el servidor tiene varias unidades, es posible que deba configurar las opciones del BIOS.

La configuración de arranque del BIOS determina la manera en que se arranca el servidor. Por lo general, el dispositivo de CD-ROM se muestra primero en la lista.

Nota Si usa ESXi integrado, la configuración de arranque del BIOS determina si el servidor se inicia desde un dispositivo de arranque de ESXi o desde otro dispositivo de arranque. Por lo general, el dispositivo flash USB se muestra primero en la lista de la configuración de arranque del BIOS en la máquina que aloja ESXi.

Cuando instala o actualiza ESXi en modo UEFI, el instalador crea una opción de arranque UEFI denominada VMware ESXi y la convierte en la opción de arranque predeterminada, por lo que no es necesario cambiar el orden de arranque.

Es posible cambiar la configuración de arranque configurando el orden de arranque en el BIOS durante el inicio o seleccionado un dispositivo de arranque desde el menú selección de dispositivos de arranque. Cuando se cambia el orden de arranque en el BIOS, la nueva configuración afecta todos los reinicios posteriores. Cuando se selecciona un dispositivo de arranque desde el menú selección de dispositivos de arranque, la selección afecta únicamente el arranque actual.

Algunos servidores no incluyen un menú selección de dispositivos de arranque, en cuyo caso se debe cambiar el orden de arranque en el BIOS incluso para los arranques únicos y, a continuación, se debe volver a cambiar durante un reinicio posterior.

Cómo cambiar la configuración de arranque del BIOS para ESXi

Ajuste la configuración de arranque del BIOS para ESXi si desea que el servidor arranque en ESXi de forma predeterminada.

Las versiones ESXi Instalable y ESXi Integrada, no pueden existir en el mismo host.

Procedimiento

1 Mientras se enciende el host ESXi, presione la tecla necesaria para entrar en la configuración del BIOS del host.

   En función del hardware del servidor, la tecla podría ser una tecla de función o Suprimir. La opción para entrar a la configuración del BIOS podría ser diferente para su servidor.

2 Seleccione la configuración de arranque del BIOS.

Opción	Descripción
Si está utilizando la versión instalable de ESXi	Seleccione el disco en el que instaló el software ESXi y muévalo a la primera posición de la lista. El host arrancará en ESXi.
Si está utilizando la versión integrada de ESXi	Seleccione el dispositivo flash USB y muévalo a la primera posición de la lista. El host arrancará en el modo ESXi.

Configuración de la opción de arranque para medios virtuales

Si usa software de administración remota para configurar ESXi, es posible que deba configurar la opción de arranque para medios virtuales.

Los medios virtuales son una manera de conectar un medio de almacenamiento remoto como CD-ROM, dispositivo de almacenamiento USB, imagen ISO y disquete con un servidor de destino que puede estar en cualquier lado de la red. El servidor de destino tiene acceso al medio remoto, y puede leerlo y escribir en él como si estuviera conectado físicamente al puerto USB del servidor.

Requisitos previos

Las versiones ESXi Instalable y ESXi Integrada, no pueden existir en el mismo host.

Procedimiento

1 Conecte el medio al dispositivo virtual.

   Por ejemplo, si utiliza un servidor Dell, inicie sesión en Dell Remote Access Controller (DRAC) o una interfaz de administración remota similar y seleccione una unidad de disquete o CD-ROM física, o bien proporcione una ruta de acceso a una imagen de disquete o de CD-ROM.

2 Reinicie el servidor.

3 Mientras se enciende el servidor, entre al menú de selección de dispositivos.

   En función del hardware del servidor, la tecla podría ser una tecla de función o Suprimir.

4 Siga las instrucciones para seleccionar el dispositivo virtual.

Resultados

El servidor arranca desde el dispositivo configurado una vez y vuelve al orden de arranque predeterminado en los arranques subsiguientes. Al instalar o actualizar ESXi en modo UEFI, no es necesario cambiar el orden de arranque, ya que el orden de arranque predeterminado del sistema está establecido en VMware ESXi.

Configuración de las opciones de red

ESXi requiere una dirección IP para la red de administración. Para configurar las opciones de red básicas, utilice vSphere Client o la consola directa.

Utilice vSphere Client si está conforme con la dirección IP asignada por el servidor DHCP.

Utilice la consola directa para la configuración de red en los casos siguientes:

- Si no está conforme con la dirección IP asignada por el servidor DHCP.
- Si no está autorizado para emplear la dirección IP asignada por el servidor DHCP.
- Si ESXi no tiene una dirección IP. Esta situación podría darse si en la fase de configuración automática no se configuró DHCP correctamente.
- Si se seleccionó el adaptador de red incorrecto durante la fase de configuración automática.

Utilice los comandos ESXCLI para configurar los ajustes de red. Consulte comandos de red esxcli.

Acceso de red a un host ESXi

El comportamiento predeterminado es configurar la red de administración ESXi con DHCP. Puede anular el comportamiento predeterminado y utilizar una configuración de IP estática para la red de administración después de que se complete la instalación.

Tabla 4-21. Situaciones de configuración de red compatibles con ESXi

Situación	Enfoque
Debe aceptar la configuración de IP ajustada por DHCP.	En la consola directa de ESXi, puede buscar la dirección IP asignada a través de DHCP a la interfaz de administración de ESXi. Puede utilizar esa dirección IP para conectarse al host desde vSphere Client y personalizar la configuración, incluido el cambio de la dirección IP de administración.
Una de las siguientes situaciones es real: ■ No tiene un servidor DHCP. ■ El host ESXi no está conectado a un servidor DHCP. ■ El servidor DHCP conectado no funciona de forma correcta.	Durante la fase de configuración automática, el software asigna la dirección IP local de vínculo, que se encuentra en la subred 169.254.x.x/16. La dirección IP asignada aparece en la consola directa. Puede anular la dirección IP local de vínculo mediante la configuración de una dirección IP estática a través de la consola directa.
El host ESXi se conecta a un servidor DHCP en funcionamiento, pero no desea utilizar la dirección IP configurada por DHCP.	Durante la fase de configuración automática, el software asigna una dirección IP configurada por DHCP. Puede realizar la conexión inicial a través de la dirección IP configurada por DHCP. A continuación, puede configurar una dirección IP estática. Si posee un acceso físico al host ESXi, puede anular la dirección IP configurada por DHCP mediante la configuración de una dirección IP estática a través de la consola directa.
Sus directivas de implementación de seguridad no permiten que se enciendan hosts sin configuración en la red.	Siga el procedimiento de configuración en Configurar la red en un host que no se haya adjuntado a la red.

Recomendaciones de seguridad para redes de ESXi

El aislamiento del tráfico de red es fundamental para proteger el entorno de ESXi. Las distintas redes requieren diferente acceso y nivel de aislamiento.

El host ESXi usa varias redes. Emplee las medidas de seguridad que correspondan para cada red y aísle el tráfico de aplicaciones y funciones específicas. Por ejemplo, asegúrese de que el tráfico de VMware vSphere® vMotion® no pase por redes en las que haya máquinas virtuales. El aislamiento impide las intromisiones. Además, por motivos de rendimiento, también se recomienda usar redes separadas.

- Las redes de infraestructura de vSphere se usan para funciones como vSphere vMotion, VMware vSphere Fault Tolerance, VMware vSAN y almacenamiento. Aísle estas redes según sus funciones específicas. Generalmente, no es necesario dirigir estas redes fuera de un rack de servidor físico único.
- Una red de administración aísla los distintos tráficos (tráfico de clientes, de la interfaz de la línea de comandos (CLI) o de la API, y del software de terceros) de otros tráficos. En general, solo los administradores de sistemas, redes y seguridad pueden acceder a la red de administración. Para proteger el acceso a la red de administración, utilice un host bastión o una red privada virtual (VPN). Controle estrictamente el acceso dentro de esta red.

- El tráfico de las máquinas virtuales puede transmitirse por medio de una red o de muchas. Puede optimizar el aislamiento de las máquinas virtuales mediante soluciones de firewall virtuales que establezcan reglas de firewall en la controladora de red virtual. Esta configuración se envía junto con una máquina virtual cuando esta se migra de un host a otro dentro del entorno de vSphere.

Selección de los adaptadores de red para la red de administración

El tráfico entre un host ESXi y cualquier software de administración externo se transmite por medio de un adaptador de red Ethernet en el host. Puede usar la consola directa para elegir los adaptadores de red que utiliza la red de administración.

El software de administración externo incluye, entre otros, vCenter Server y el cliente SNMP. A los adaptadores de red en el host se les asigna el nombre vmnic*N*, donde N es un número único que identifica el adaptador de red (por ejemplo, vmnic0, vmnic1 y así sucesivamente).

Durante la fase de configuración automática, el host ESXi selecciona vmnic0 para el tráfico de administración. Puede anular la opción predeterminada seleccionando manualmente el adaptador de red que transmite el tráfico de administración para el host. En algunos casos, se recomienda usar un adaptador de red Gigabit Ethernet para el tráfico de administración. Otra manera de ayudar a garantizar la disponibilidad es seleccionar varios adaptadores de red. El uso de varios adaptadores de red permite las funcionalidades de equilibrio de la carga y conmutación por error.

Procedimiento

1 Desde la consola directa, seleccione **Configurar red de administración** y presione Intro.

2 Seleccione **Adaptadores de red** y presione Intro.

3 Seleccione un adaptador de red y presione Intro.

Resultados

Una vez que la red esté en funcionamiento, puede usar vSphere Client para conectar ESXi al host mediante vCenter Server.

Configurar el id. de VLAN

Puede establecer el número de identificador de LAN virtual (VLAN) del host ESXi.

Procedimiento

1 Desde la consola directa, seleccione **Configurar red de administración** y presione Intro.

2 Seleccione **VLAN** y presione Intro.

3 Introduzca un número de identificador de VLAN del 1 al 4094.

Configurar IP para ESXi

De forma predeterminada, DHCP establece la dirección IP, la máscara de subred y la puerta de enlace predeterminada.

Para futuras referencias, anote la dirección IP.

Para que DHCP funcione, el entorno de red debe tener un servidor DHCP. Si DHCP no está disponible, el host asigna la dirección IP local del vínculo, que se encuentra en la subred 169.254.x.x/16. La dirección IP asignada aparece en la consola directa. Si no cuenta con acceso al host a través de monitor físico, puede acceder a la consola directa mediante una aplicación de administración remota. Consulte Usar aplicaciones de administración remota

Si tiene acceso a la consola directa, cuenta con la opción de configurar una dirección de red estática. La máscara de red predeterminada es 255.255.0.0.

Configurar IP desde la consola directa

Si tiene acceso físico al host o acceso remoto a la consola directa, puede usar la consola directa para configurar la dirección IP, la máscara de subred y la puerta de enlace predeterminada.

Procedimiento

1 Seleccione **Configurar red de administración** y presione Intro.

2 Seleccione **Configuración IP** y presione Intro.

3 Seleccione **Establecer dirección IP estática y configuración de red**.

4 Introduzca la dirección IP, la máscara de subred y la puerta de enlace predeterminada y presione Intro.

Configurar IP desde vSphere Client

Si no tiene acceso físico al host, puede utilizar vSphere Client para establecer la configuración de IP estática.

Procedimiento

1 Inicie sesión en vCenter Server desde vSphere Client.

2 Seleccione el host en el inventario.

3 En la pestaña **Configurar**, expanda **Redes**.

4 Seleccione **Adaptadores de VMkernel**.

5 Seleccione **Red de administración vmk0** y haga clic en el icono de edición.

6 Seleccione **Configuración de IPv4**.

7 Seleccione **Usar configuración de IPv4 estática**.

8 Introduzca o modifique la configuración de la dirección IPv4 estática.

9 (opcional) Configure direcciones IPv6 estáticas.

   a Seleccione **Configuración de IPv6**.

   b Seleccione **Direcciones IPv6 estáticas**.

   c Haga clic en el icono de adición.

   d Escriba la dirección IPv6 y haga clic en **Aceptar**.

10 Haga clic en **Aceptar**.

Configurar DNS para ESXi

Puede seleccionar una configuración de DNS manual o automática del host ESXi.

El valor predeterminado es automático. Para que el DNS funcione, su entorno de red debe tener un servidor DHCP y un servidor DNS.

En entornos de red donde no hay DNS automático o no se desea que haya uno, puede configurar información de DNS estático, incluidos un nombre de host, un servidor de nombres principal, un servidor de nombres secundario y sufijos DNS.

Configurar DNS desde la consola directa

Si tiene acceso físico al host o acceso remoto a la consola directa, puede usar la consola directa para configurar información de DNS.

Procedimiento

1 Seleccione **Configurar red de administración** y presione Intro.

2 Seleccione **Configuración del DNS** y presione Intro.

3 Seleccione **Usar las siguientes direcciones de servidor DNS y nombre de host**.

4 Introduzca el servidor principal, el servidor alternativo (opcional) y el nombre de host.

Configurar sufijos DNS

Si tiene acceso físico al host, puede utilizar la consola directa para configurar la información del DNS. De forma predeterminada, DHCP adquiere los sufijos DNS.

Procedimiento

1 Desde la consola directa, seleccione **Configurar la red de administración**.

2 Seleccione **Personalizar sufijos DNS** y presione Intro.

3 Introduzca los nuevos sufijos DNS.

Configurar la red en un host que no se haya adjuntado a la red

Algunos entornos altamente seguros no permiten que se enciendan hosts no configurados en la red. Puede configurar el host antes de conectarlo a la red.

Requisitos previos

Compruebe que no existan cables de red conectados al host.

Procedimiento

1 Encienda el host.

2 Utilice la interfaz de usuario de la consola directa para configurar la contraseña para la cuenta de administrador (raíz).

3 Utilice la interfaz de usuario de la consola directa para configurar una dirección IP estática.

4 Conecte un cable de red al host.

5 (opcional) Utilice vSphere Client para conectarse a un sistema vCenter Server.

6 (opcional) Agregue el host al inventario de vCenter Server.

Probar la red de administración

Puede usar la consola directa para realizar pruebas de conectividad de red sencillas.

La consola directa realiza las siguientes pruebas.

- Hace ping en la puerta de enlace predeterminada
- Hace ping en el servidor de nombre del DNS principal
- Hace ping en el servidor de nombre del DNS secundario
- Resuelve el nombre de host configurado

Procedimiento

1 Desde la consola directa, seleccione **Probar red de administración** y presione Intro.

2 Presione Intro para comenzar la prueba.

Reiniciar los agentes de administración

Los agentes de administración sincronizan los componentes de VMware y permiten acceder al host ESXi mediante vSphere Client y vCenter Server.

vSphere Client y vCenter Server se instalan con el software de vSphere. Es posible que necesite reiniciar los agentes de administración si se interrumpe el acceso remoto. Al reiniciar los agentes de administración, se reinician todos los agentes de administración y los servicios que están instalados y se ejecutan en `/etc/init.d` en el host ESXi. Generalmente, estos agentes incluyen hostd, ntpd, sfcbd, slpd, wsman y vobd. El software también reinicia Fault Domain Manager (FDM) si está instalado.

Los usuarios que accedan a este host a través de vSphere Client y vCenter Server perderán la conectividad cuando reinicie los agentes de administración.

Procedimiento

1 Desde la consola directa, seleccione **Opciones de solución de problemas** y presione Intro.

2 Seleccione **Reiniciar agentes de administración** y presione Intro.

3 Presione F11 para confirmar el reinicio.

Resultados

El host ESXi reiniciará los servicios y los agentes de administración.

Reiniciar la red de administración

Puede que sea necesario reiniciar la interfaz de red de administración para restaurar la red o renovar una concesión de DHCP.

Si se reinicia la red de administración, se produce una breve interrupción de red que puede afectar temporalmente a las máquinas virtuales en ejecución.

Si una concesión de DHCP renovada provoca una nueva identidad de red (dirección IP o nombre de host), se desconecta el software de administración remota.

Procedimiento

1 Desde la consola directa, seleccione **Reiniciar red de administración** y presione Intro.

2 Presione F11 para confirmar el reinicio.

Prueba de la conectividad con los dispositivos y las redes

Puede utilizar la consola directa para realizar algunas pruebas de conectividad de red simples y especificar otros dispositivos y redes.

Procedimiento

1 Desde la consola directa, seleccione **Probar red de administración** y presione Intro.

2 Escriba las direcciones a las que desee emitir un ping u otro nombre de host DNS que desee resolver.

3 Presione Intro para comenzar la prueba.

Restauración del conmutador estándar

vSphere Distributed Switch funciona como un único conmutador virtual en todos los hosts asociados.

Las máquinas virtuales pueden mantener una configuración de red coherente cuando se migran a varios hosts. Si se migra un conmutador estándar existente, o un adaptador virtual, a un conmutador distribuido y este se vuelve innecesario o deja de funcionar, puede restaurar el conmutador estándar para asegurarse de que el host siga siendo accesible. Cuando se restaura el conmutador estándar, se crea un nuevo adaptador virtual y el vínculo superior de la red de administración que está conectado actualmente al conmutador distribuido se migra al nuevo conmutador virtual.

Es posible que necesite restaurar el conmutador estándar por las siguientes razones:

- Distributed Switch no se necesita o no funciona.
- Es necesario reparar Distributed Switch para restaurar la conectividad con vCenter Server y los hosts deben permanecer accesibles.

- No es deseable que vCenter Server administre el host. Cuando el host no está conectado a vCenter Server, la mayoría de las características de Distributed Switch no están disponibles para el host.

Requisitos previos

Compruebe que la red de administración esté conectada a un conmutador distribuido.

Procedimiento

1 En la consola directa, seleccione **Restaurar conmutador estándar** y presione Intro.

   Si el host se encuentra en un conmutador estándar, la opción aparece atenuada y no puede seleccionarla.

2 Presione F11 para confirmar.

Configurar el registro del sistema

Los hosts ESXi ejecutan el servicio Syslog (`vmsyslogd`) que escribe mensajes de componentes del sistema en archivos de registro y puede reenviar mensajes a recopiladores de Syslog.

Puede configurar la cantidad y la ubicación de los registros. También puede crear y aplicar filtros de registro para modificar la directiva de registro de un host ESXi.

Al configurar hosts remotos para syslog, también debe abrir algunos puertos especificados en el firewall del host ESXi para permitir la transmisión de mensajes de registro. Para obtener más información, consulte Apertura del firewall para la emisión de Syslog en hosts remotos.

Configurar Syslog en hosts ESXi

Puede utilizar vSphere Client, VMware Host Client o el comando `esxcli system syslog` para configurar el servicio syslog.

El servicio Syslog recibe, clasifica y almacena mensajes de registro para análisis que le ayudarán a tomar medidas preventivas en su entorno.

Establezca Syslog de ESXi mediante vSphere Client

Puede usar el comando vSphere Client para configurar el servicio Syslog de forma global y editar varias opciones avanzadas.

Procedimiento

1 Desplácese hasta el host ESXi en el inventario de vSphere Client.

2 Haga clic en **Configurar**.

3 En **Sistema**, haga clic en **Configuración avanzada del sistema**.

4 Haga clic en **Editar**.

5 Filtre por **`syslog`**.

6 Para configurar globalmente el registro y configurar varias opciones avanzadas, consulte Opciones de Syslog de ESXi.

7 (opcional) Para sobrescribir los valores predeterminados de tamaño de registro y rotación de registros de cualquier registro:

   a Haga clic en el nombre del registro que desea personalizar.

   b Introduzca el número de rotaciones y el tamaño de registro que desea.

8 Haga clic en **Aceptar**.

Resultados

Los cambios en las opciones de syslog surten efecto.

Nota La configuración de parámetros de Syslog que se define mediante vSphere Client o VMware Host Client se aplica inmediatamente. Sin embargo, la mayoría de los ajustes que se definen mediante ESXCLI requieren un comando adicional para que surtan efecto. Para obtener más información, consulte Opciones de Syslog de ESXi.

Establezca Syslog de ESXi mediante VMware Host Client

Puede utilizar VMware Host Client para configurar y editar parámetros de servicio de Syslog en hosts ESXi.

Procedimiento

1 En VMware Host Client, en **Host**, haga clic en **Administrar > Sistema > Configuración avanzada**.

2 En el panel **Buscar**, escriba una configuración de Syslog que desee definir. Consulte Opciones de Syslog de ESXi.

3 Seleccione la opción y haga clic en **Editar opción**.

4 Establezca el valor como se describe en la tabla de parámetros de Opciones de Syslog de ESXi.

5 Haga clic en **Guardar**.

Establecer Syslog ESXi mediante ESXCLI

Puede configurar el servicio Syslog en hosts ESXi mediante el comando ESXCLI: `esxcli system syslog config set <syslog option>`.

Requisitos previos

Para obtener información sobre el uso del comando esxcli system syslog y otros comandos de ESXCLI, consulte Introducción a ESXCLI. Para obtener más información sobre cómo abrir el firewall de ESXi para el puerto definido en cada especificación de host remoto, consulte Configurar el firewall de ESXi.

Nota El uso de ESXCLI requiere que ESXi abra los inicios de sesión SSH, lo cual supone un riesgo de seguridad y no se recomienda. Si decidió utilizar ESXCLI, asegúrese de utilizar el comando `esxcli system syslog reload` después de configurar cada parámetro para asegurarse de que se aplique.

Procedimiento

- Utilice el comando ESXCLI `esxcli system syslog config set <syslog option>` para establecer una opción de Syslog que decida habilitar. Por ejemplo, para establecer la opción `Syslog.global.logHost`, utilice el comando `esxcli system syslog config set --loghost=<str>`

  Después de configurar `Syslog.global.logHost`, los hosts ESXi abren y mantienen las conexiones con los recopiladores de Syslog, y la transmisión de mensajes comienza inmediatamente. Cuando ESXi genera un mensaje de Syslog, lo escribe en el archivo de registro adecuado en el host ESXi y también lo reenvía a todos los recopiladores de Syslog configurados.

Ajustar syslog en hosts ESXi

Al utilizar la configuración de Syslog correcta, puede lograr una supervisión proactiva del entorno, reducir el tiempo de inactividad y tomar medidas preventivas en los servidores.

Al configurar syslog, debe tener en cuenta varios parámetros que afectan a la retención de archivos de registro, la transmisión de syslog, la longitud de la transmisión, el control de errores y la configuración de certificados SSL para la transmisión segura de mensajes de syslog. A continuación se muestran recomendaciones para ajustar los parámetros de syslog. Puede ver una descripción de todos los parámetros disponibles en Opciones de Syslog de ESXi.

Cómo especificar la retención de archivos de registro

De forma predeterminada, los archivos de registro no pueden expandirse más allá de un tamaño configurado. Una vez que un archivo de registro alcanza el tamaño configurado, el registro se enruta a un nuevo archivo de registro y se elimina el archivo de registro más antiguo.

Nota La práctica recomendada es equilibrar los ajustes de rotación y tamaño. Aumentar el ajuste de rotación garantiza que los archivos syslog se generen con la frecuencia suficiente para evitar daños o destrucción potenciales en los otros archivos de registro. Aumentar el ajuste de tamaño reduce el tiempo necesario para cambiar a otro archivo de registro. El ajuste de tamaño óptimo es un múltiplo de 1024 KiB.

Utilice el ajuste `Syslog.global.defaultSize` para especificar el tamaño máximo del archivo de registro en KiB y `Syslog.global.defaultRotate` para establecer el número máximo de archivos de registro antiguos que se deben conservar antes de rotar a un nuevo archivo de registro. Para cambiar los parámetros de retención de archivos de registro asociados a un programa específico, utilice `Syslog.loggers.<progName>.rotate` y `Syslog.loggers.<progName>.size settings`, donde `<progName>` es el nombre del programa cuyos parámetros desea ajustar.

Administrar la configuración que afecta al archivo de registro de la máquina virtual

Puede configurar algunas opciones que afectan al archivo de registro de la máquina virtual (`vmware.log`) en el archivo `vmx` o en el archivo `/etc/vmware/config`. Debe apagar una máquina virtual para editar el archivo `vmx` y las ediciones solo surtirán efecto en esa máquina virtual. Si utiliza el archivo `/etc/vmware/config`, debe agregar el prefijo *"vmx"* a la configuración, por ejemplo `vmx.log.keepOld = "20"`, y las modificaciones afectan a todas las máquinas virtuales del host ESXi.

Tabla 4-22. Opciones configurables para el archivo vmware.log

Parámetro	Descripción	Ejemplo	Notas
`logging`	Deshabilita el registro de todas las máquinas virtuales.	El valor predeterminado es `logging = "TRUE"`. Para deshabilitar el registro de máquinas virtuales: `logging = "FALSE"`	No utilice esta configuración, ya que, al deshabilitar el registro de máquinas virtuales, resulta extremadamente difícil o imposible obtener soporte para los problemas de la máquina virtual. Si necesita utilizar esta opción por algún motivo, solo puede colocarla en el archivo `vmx` de una máquina virtual.

`log.throttleBytesPerSec`	Controla cuándo se regula un archivo de registro.
	La regulación de archivos de registro se produce cuando las escrituras en el archivo `vmware.log` superan la velocidad especificada durante una cantidad significativa de tiempo. Esto ocurre cuando el código dentro del proceso VMX, el cual controla una máquina virtual, crea demasiados mensajes de registro. El valor predeterminado para esta opción es 1 KB/s.
	En el caso de que se regule el registro, verá <<< `Log Throttled` >>> en el archivo `vmware.log`.
		`log.throttleBytesPerSec = "1500"`
		Para deshabilitar la regulación del registro, utilice
		`log.throttleBytesPerSec = "0xFFFFFFFF"`
			La regulación del archivo de registro puede ocultar la información necesaria para diagnosticar problemas con la máquina virtual afectada. Si necesita deshabilitar la regulación de registros, coloque la línea del ejemplo en el archivo `vmx` de la máquina virtual afectada. Elimine la línea una vez que finalice la sesión de depuración.

`log.keepOld`	Controla el número de archivos `vmware.log` antiguos que se conservarán.	`log.keepOld = "20"`	No coloque el valor de esta opción por debajo del valor predeterminado (10). Si las máquinas virtuales se modifican o mueven con frecuencia, considere la posibilidad de aumentar esta opción a 20 o más.

Tabla 4-22. Opciones configurables para el archivo vmware.log (continuación)

Parámetro	Descripción	Ejemplo	Notas

`log.rotateSize`	Controla el tamaño máximo de un archivo `vmware.log` en bytes.	`log.rotateSize = "2500000"`
		Para deshabilitar la limitación del tamaño máximo de un archivo `vmware.log`, utilice
		`log.rotateSize = "0"`
			Un valor de esta opción inferior a 100.000 puede provocar la pérdida de mensajes de registro críticos y afectar al rendimiento de la máquina virtual. En ESXi 7.x y versiones anteriores, el valor predeterminado de esta opción no establece ningún límite en el tamaño de un archivo `vmware.log`. En ESXi 8.x y versiones posteriores, el valor predeterminado de esta opción es 2.048.000.

`log.fileName`	Controla el nombre y la ubicación de los archivos de registro de la máquina virtual.	`log.fileName = "myVMLog"`
		Esta opción cambia el nombre de los archivos de registro de la máquina virtual de vmware.log a `myVMlog`.
		`log.fileName = "/vmfs/volumes/vol1/myVM/myVM.log"`
		Esta opción dirige los archivos de registro de la máquina virtual a un directorio de un volumen de VMFS diferente (vol1) al utilizar `myVM` para un nombre de archivo.
			No coloque un archivo de registro fuera del directorio de la máquina virtual para asegurarse de que la recopilación de paquetes de soporte del host seleccione el archivo de registro, el cual puede ser determinante a la hora de depurar los problemas de la máquina virtual.

Tabla 4-22. Opciones configurables para el archivo vmware.log (continuación)

Parámetro	Descripción	Ejemplo	Notas
`log.fileLevel`	Controla el nivel mínimo en el que se escriben los mensajes en `vmware.log`. Cada mensaje de registro tiene un nivel asociado a él. Los niveles inferiores a la configuración especificada no se agregan a un archivo de registro de máquina virtual. Los niveles de registro de mensajes de la máquina virtual (desde el más restringido al menos restringido) son: ■ error ■ advertencia ■ notice ■ info (valor predeterminado) ■ registro detallado ■ depuración ■ depuración1 ■ depuración2 ■ depuración3 ■ depuración4 ■ depuración5 ■ depuración6 ■ depuración7 ■ depuración8 ■ depuración9 ■ depuración10	`log.fileLevel = "debug1"`	No establezca el nivel en un nivel más restrictivo que "info" para evitar que se filtren los mensajes necesarios para depurar los problemas de la máquina virtual. Baje el nivel por debajo de "info" solo cuando lo solicite el soporte con licencia. Restaure el ajuste a "info" una vez que finalice la depuración.
`log.filter.minLogLevel.<groupName>`	Controla la salida de los mensajes de depuración especializados.	`log.filter.minLogLevel.disklib = "debug5"`	Utilice esta opción solo cuando lo solicite el equipo de soporte con licencia, el cual debe proporcionar uno o varios parámetros `<groupName>`. Elimine el ajuste una vez que finalice la depuración.

Tabla 4-22. Opciones configurables para el archivo vmware.log (continuación)

Parámetro	Descripción	Ejemplo	Notas
`log.sysogID`	Permite el envío de mensajes de registro de máquina virtual al registrador del sistema de un host ESXi, como Syslog.	`log.syslogID = "vmx"`	Utilice `"vmx"` como valor para esta opción y permitir que el daemon de syslog de ESXi, `vmsyslogd`, envíe estos mensajes a un archivo de registro independiente.
`log.syslogLevel`	Controla el nivel mínimo en el cual se envían los mensajes al registrador del sistema de un host ESXi, como Syslog.	`log.syslogLevel = "debug"`	Los niveles y el funcionamiento de esta opción son idénticos a los de la opción `log.fileLevel`.

Cómo especificar la transmisión de mensajes a hosts remotos

Opcionalmente, puede configurar ESXi para que envíe mensajes de syslog a uno o varios hosts remotos, denominados recopiladores de syslog, como VMware vRealize Log Insight (anteriormente vCenter Log Insight), para recopilar mensajes de syslog.

Nota La práctica recomendada es configurar cada host ESXi para que envíe mensajes de syslog al menos a un recopilador de syslog. Esto ayuda a garantizar que los mensajes se conserven en caso de que se produzca un evento catastrófico del sistema y que pueda procesar mensajes de Syslog de diferentes maneras, como la categorización y el análisis en tiempo real (por ejemplo, por tipo, intervalo de tiempo o máquina), o archivar mensajes.

Utilice el ajuste de `Syslog.global.logHost` para definir las especificaciones del host remoto. Separe las especificaciones de varios hosts remotos con una coma (,). Después de configurar `Syslog.global.logHost`, los hosts ESXi abren y mantienen las conexiones con los recopiladores de syslog, y la transmisión de mensajes comienza inmediatamente. Cuando ESXi genera un mensaje de syslog, lo escribe en el archivo de registro adecuado en el host ESXi y también lo reenvía a todos los recopiladores de syslog configurados.

Además de los mensajes de syslog, también se pueden transmitir mensajes de auditoría a los recopiladores de syslog por motivos de seguridad. Los registros de auditoría realizan un seguimiento de la actividad relacionada con la seguridad en el host ESXi. Para obtener más información sobre los registros de auditoría, consulte Registros de auditoría.

Nota Consulte con el equipo de respuesta de seguridad de su empresa si hay que establecer registros de auditoría y cómo hacerlo. Por lo general, las configuraciones certificadas requieren que se habiliten los registros de auditoría.

Lo que sigue es la sintaxis para especificaciones de host remoto de `Syslog.global.logHost` :

```
protocol://target[:port]
```

Parámetro	Descripción	Notas
protocol	Especifica el protocolo de red. Los valores válidos son udp, tcp y ssl.	El protocolo ssl especifica que la transmisión de mensajes de syslog está cifrada. Los protocolos tcp y udp no cifran la transmisión. **Nota** Si la captura de mensajes de syslog o de auditoría es crucial para el sistema, evite utilizar el protocolo udp porque la infraestructura de redes externa a ESXi puede descartar mensajes UDP.
target	Especifica el host remoto. Puede utilizar una dirección IPV4 o IPv6 o un nombre de host.	Cuando utilice una dirección IPV6, debe insertarla entre corchetes [xxx], donde xxx es la dirección IPV6.
port	(Opcional) Especifica el puerto de host remoto que se utilizará. Si utiliza UDP o TCP. El puerto predeterminado es 1514. Si utiliza SSL. El puerto predeterminado es 514. Si decide utilizar puertos diferentes a 514 o 1514, debe ajustar el ESXi Firewall para abrir el puerto.	Para obtener más información sobre cómo abrir el firewall de ESXi para el puerto definido en cada especificación de host remoto, consulte Configurar el firewall de ESXi.

Ejemplos de especificaciones de máquina remota:

Ejemplo de cadena syslog.global.logHost	Notas
tcp://10.176.130.7:12345	Transmite mensajes de syslog a 10.176.130.7 mediante TCP/IP y el puerto 12345.
tcp://[2001:db8:85a3:8d3:1319:8a2e:370:7348]	Transmite mensajes de syslog a una dirección IPV6 mediante el puerto 1514.
tcp://[2001:db8:85a3:8d3:1319:8a2e:370:7348]:5432	Transmita mensajes de syslog a una dirección IPV6 mediante el puerto 54321.
udp://company.com	Transmite mensajes de syslog a company.com mediante UDP y el puerto 514.
udp://company.com,tcp://10.20.30.40:1050	Transmite mensajes de syslog a dos hosts remotos. El primer host remoto utiliza UDP para comunicarse con company.com mediante el puerto 514. El segundo host remoto utiliza TCP para comunicarse con la dirección IPV4 10.20.30.40 mediante el puerto 1050.
ssl://company.com	Transmite mensajes de syslog a company.com mediante SSL (TLS) y el puerto 514.

Longitud máxima de transmisión de mensajes

Si utiliza UDP, la longitud máxima de transmisión de mensajes de syslog es de 480 bytes para IPV4 y de 1180 bytes para IPV6.

Para TCP o SSL, la longitud máxima predeterminada de transmisión de mensajes de syslog es de 1 kibibyte (KiB). Puede aumentar esta longitud con el parámetro `Syslog.global.remoteHost.maxMsgLen`. El valor máximo es 16 KiB. Los mensajes de más de 16 KiB se truncan.

Nota Si es necesario aumentar la longitud máxima de transmisión, la práctica recomendada es aumentar la longitud solo lo específicamente necesario.

Aumentar la longitud máxima de los mensajes de syslog puede causar problemas si la infraestructura de redes y syslog externa a ESXi no puede controlar mensajes de más de 1 KiB.

Nota La práctica recomendada es no utilizar UDP para transmitir mensajes de syslog debido a las restricciones de longitud de paquetes y a la posibilidad de que la infraestructura de redes externas descarte los mensajes.

Consideraciones para los certificados al configurar transmisiones SSL a hosts remotos

Al configurar ESXi para transmitir mensajes de syslog a hosts remotos con SSL, debe agregar un certificado SSL para cada host remoto al almacén de CA de host ESXi. Para obtener más información, consulte Administrar certificados para hosts ESXi y Administrar certificados de CA con ESXCLI.

Nota Consulte la documentación de Syslog Collector sobre cómo configurar el recopilador para la recepción segura de mensajes de syslog mediante SSL y una clave privada.

Parámetros adicionales de transmisión de SSL

Un sistema ESXi que cumpla con los requisitos de certificación de seguridad puede requerir la habilitación de comprobaciones de X509 CRL. Para activar la configuración avanzada de `Syslog.global.certificate.strictX509Compliance` y `Syslog.global.certificate.checkCRL`, cambie el valor predeterminado de `false` a `true`. Debido a las limitaciones de implementación, si se habilitan las comprobaciones de CRL mediante la opción `Syslog.global.certificate.checkSSLCerts`, todos los certificados de una cadena de certificados deben proporcionar un vínculo de CRL. De forma predeterminada, la opción está habilitada. Puede desactivar las comprobaciones de certificados SSL si cambia el valor a `false`, pero esta no es una práctica recomendada. Es posible que deba desactivar las comprobaciones de certificados SSL al solucionar problemas de comunicación con un host remoto, pero solo durante un tiempo limitado.

Dónde encontrar la información del estado y el error del daemon de syslog

El daemon de syslog de ESXi utiliza el archivo de registro `/var/run/log/vmsyslogd.log` para almacenar información sobre el estado y los errores, incluidos los mensajes descartados. Si la transmisión de registros de auditoría está habilitada, el daemon de syslog también emite registros de auditoría relacionados con su funcionamiento, como las condiciones de inicio, detención y error del daemon, lo que le permite comprobar que el daemon de syslog se ejecute correctamente.

Cómo cambiar el área predeterminada de almacenamiento de archivos de registro de syslog

El área predeterminada de almacenamiento de archivos de registro de syslog es `/var/run/log`, local para cada host ESXi. Utilice la variable de configuración de syslog `Syslog.global.logDir` para cambiar el área predeterminada de almacenamiento de archivos de registro de syslog, siempre y cuando la ubicación resida en el almacenamiento persistente. Si `Syslog.global.logDir` se configura en un almacén persistente compartido por varios hosts ESXi para almacenar los archivos de registro de syslog, cambie el valor de `Syslog.global.logDirUnique` a `true` para que no se mezclen los registros. La opción `Syslog.global.logDirUnique` garantiza que cada máquina ESXi obtenga un nombre único que se agrega a la ruta `Syslog.global.logDir`, separando los archivos de registro de otros hosts.

Cola de mensajes de syslog para hosts remotos y descarte de mensajes

Una vez que se inician las emisiones de Syslog, nunca se detienen, excepto para reinicios y errores de ESXi, o una reconfiguración de Syslog para detenerse.

ESXi utiliza un mecanismo de cola basado en memoria con capacidad limitada para transmitir mensajes de Syslog y registros de auditoría a hosts remotos. Este mecanismo permite que el servicio `vmsyslogd` controle ráfagas cortas de mensajes o problemas de conectividad de red que se resuelven rápidamente sin necesidad de descartar datos.

Cuando los problemas de conectividad duran más tiempo o el flujo de datos entrantes supera continuamente el límite que puede tolerar el mecanismo de cola, el servicio `vmsyslogd` descarta algunos mensajes de Syslog.

Para que estos descartes sean los mínimos posibles, coloque los archivos de registro de `vmsyslogd` en el almacenamiento disponible más rápido y configure los recopiladores de Syslog en una red con un ancho de banda de extremo a extremo igual o superior a 1 GigE.

Si ve demasiados registros procedentes de una aplicación, realice una solicitud de servicio de soporte para su análisis y corrección.

Puede ver las estadísticas sobre los descartes de mensajes en el archivo de registro del daemon de syslog.

Puede ver los mensajes descartados en `/var/run/log/vmsyslogd-dropped.log`. Este archivo de registro tiene ajustes de retención específicos, similares a los de los parámetros de retención específicos del programa. Los parámetros de retención de archivos de registro de mensajes descartados son: `Syslog.global.droppedMsgs.fileRotate` y `Syslog.global.droppedMsgs.fileSize`.

Opciones de Syslog de ESXi

Puede definir el comportamiento de las transmisiones y los archivos de syslog de ESXi mediante un conjunto de opciones de syslog.

Además de la configuración básica, como `Syslog.global.logHost`, a partir de ESXi 7.0 Update 1, hay disponible una lista de opciones avanzadas para las personalizaciones y el cumplimiento de NIAP.

Nota Configure siempre el almacenamiento persistente antes de establecer alguno de los parámetros de registro de auditoría o el parámetro de `Syslog.global.logDir`.

Nota Todos los ajustes del registro de auditoría que comienzan por `Syslog.global.auditRecord` se aplican inmediatamente. Sin embargo, para otros ajustes que defina mediante ESXCLI, asegúrese de ejecutar el comando `esxcli system syslog reload` para habilitar los cambios.

Tabla 4-23. Opciones de Syslog heredadas

<table>
<tr><th>Opción</th><th>Comando ESXCLI</th><th>Descripción</th></tr>
<tr><td>Syslog.global.logHost</td><td>esxcli system syslog config set --loghost=<str></td><td>Define una lista delimitada por comas de hosts remotos y especificaciones para transmisiones de mensajes.
Si el campo loghost=<str> está en blanco, no se reenvía ningún registro. Si bien no existe un límite estricto para la cantidad de hosts remotos que recibirán mensajes de Syslog, una buena práctica es mantener el número de hosts remotos en cinco o menos.
El formato de una especificación de host remoto es: protocol://hostname|ipv4|'['ipv6']'[:port]. El protocolo debe ser TCP, UDP o SSL. El valor de los puertos puede ser cualquier número decimal entre 1 y 65535. Si no se proporciona un puerto, SSL y TCP utilizan 1514. UDP utiliza 514. Por ejemplo: ssl://hostName1:1514.</td></tr>
<tr><td>Syslog.global.defaultRotate</td><td>esxcli system syslog config set --default-rotate=<long></td><td>Número máximo de archivos de registro antiguos que se conservarán. Puede configurar este número en forma global y para subregistradores individuales (consulte Syslog.global.defaultSize).</td></tr>
<tr><td>Syslog.global.defaultSize</td><td>esxcli system syslog config set --default-size=<long></td><td>Tamaño predeterminado de los archivos de registro, en KiB. Una vez que un archivo alcanza el tamaño predeterminado, el servicio de Syslog crea un nuevo archivo. Puede configurar este número en forma global y para subregistradores individuales.</td></tr>
</table>

Tabla 4-23. Opciones de Syslog heredadas (continuación)

Opción	Comando ESXCLI	Descripción
`Syslog.global.logDir`	`esxcli system syslog config set --logdir=<str>`	Directorio donde residen los registros. El directorio puede encontrarse en volúmenes NFS o VMFS montados. Solo el directorio `/scratch` del sistema de archivos local se mantiene en todos los reinicios. Especifique el directorio como [*nombrealmacéndatos*] *ruta_a_archivo*, donde la ruta de acceso es relativa a la raíz del volumen que respalda el almacén de datos. Por ejemplo, la ruta de acceso `[storage1] /systemlogs` se asigna a la ruta de acceso `/vmfs/volumes/storage1/systemlogs`.
`Syslog.global.logDirUnique`	`esxcli system syslog config set --logdir-unique=<bool>`	Especifica el nombre de host ESXi que se va a concatenar al valor de `Syslog.global.logDir`. Es fundamental que habilite esta opción cuando varios hosts ESXi inicien sesión en un sistema de archivos compartido. Al seleccionar esta opción, se crea un subdirectorio con el nombre del host ESXi del directorio especificado por **Syslog.global.LogDir**. Un directorio único es útil si varios hosts ESXi utilizan el mismo directorio NFS.
`Syslog.global.certificate.checkSSLCerts`	`esxcli system syslog config set --check-ssl-certs=<bool>`	Examine la comprobación de certificados SSL al transmitir mensajes a hosts remotos.

Tabla 4-24. Opciones de Syslog disponibles a partir de ESXi 7.0 Update 1

Opción	Comando ESXCLI	Descripción
`Syslog.global.auditRecord.storageCapacity`	`esxcli system auditrecords local set --size=<long>`	Especifica la capacidad del directorio de almacenamiento de registros de auditoría ubicado en el host ESXi, en MiB. No se puede reducir la capacidad del almacenamiento de registros de auditoría. Puede aumentar la capacidad antes o después de habilitar el almacenamiento de registros de auditoría (consulte `Syslog.global.auditRecord.storageEnable`).

Tabla 4-24. Opciones de Syslog disponibles a partir de ESXi 7.0 Update 1 (continuación)

Opción	Comando ESXCLI	Descripción
`Syslog.global.auditRecord.remoteEnable`	`esxcli system auditrecords remote enable`	Habilita el envío de registros de auditoría a hosts remotos. Los hosts remotos se especifican mediante el parámetro `Syslog.global.logHost`.
`Syslog.global.auditRecord.storageDirectory`	`esxcli system auditrecords local set --directory=<dir>`	Crea un directorio de almacenamiento de registros de auditoría y, a menos que se especifique, establece `/scratch/auditLog` como la ubicación predeterminada. No debe crear manualmente un directorio de almacenamiento de registros de auditoría y no puede cambiar el directorio de almacenamiento de registros de auditoría mientras esté habilitado el almacenamiento de registros de auditoría (consulte `Syslog.global.auditRecord.storageEnable`).
`Syslog.global.auditRecord.storageEnable`	`esxcli system auditrecords local enable`	Habilita el almacenamiento de registros de auditoría en un host ESXi. Si el directorio de almacenamiento de registros de auditoría no existe, se crea con la capacidad especificada por `Syslog.global.auditRecord.storageCapacity`.
`Syslog.global.certificate.checkCRL`	`esxcli system syslog config set --crl-check=<bool>`	Habilita la comprobación del estado de revocación de todos los certificados de una cadena de certificados SSL. Habilita la verificación de las CRL X.509 que no se comprueban de forma predeterminada en cumplimiento de las convenciones del sector. Una configuración validada por NIAP requiere comprobaciones de CRL. Debido a las limitaciones de implementación, si se habilitan las comprobaciones de CRL, todos los certificados de una cadena de certificados deben proporcionar un vínculo de CRL. No habilite la opción `crl-check` para instalaciones no relacionadas con la certificación, debido a la dificultad de configurar correctamente un entorno que utilice comprobaciones de CRL.

Tabla 4-24. Opciones de Syslog disponibles a partir de ESXi 7.0 Update 1 (continuación)

Opción	Comando ESXCLI	Descripción
`Syslog.global.certificate.strictX509Compliance`	`esxcli system syslog config set --x509-strict=<bool>`	Habilita la conformidad estricta con X.509. Realiza comprobaciones de validez adicionales en los certificados raíz de CA durante la verificación. Por lo general, estas comprobaciones no se realizan, ya que las raíces de CA son de confianza inherente y podrían producir incompatibilidades con las raíces de CA existentes y mal configuradas. Una configuración validada por NIAP requiere que incluso las raíces de CA pasen las validaciones. No habilite la opción `x509-strict` para instalaciones no relacionadas con la certificación, debido a la dificultad de configurar correctamente un entorno que utilice comprobaciones de CRL.
`Syslog.global.droppedMsgs.fileRotate`	`esxcli system syslog config set --drop-log-rotate=<long>`	Especifica el número de archivos antiguos de registro de mensajes descartados que se conservarán.
`Syslog.global.droppedMsgs.fileSize`	`esxcli system syslog config set --drop-log-size=<long>`	Especifica el tamaño de cada archivo de registro de mensajes descartados antes de cambiar a uno nuevo, en KiB.
`Syslog.global.logCheckSSLCerts`	`esxcli system syslog config set --check-ssl-certs=<bool>`	Examine la comprobación de certificados SSL al transmitir mensajes a hosts remotos. **Nota** Obsoleto. Use `Syslog.global.certificate.checkSSLCerts` en ESXi 7.0 Update 1 y posterior.

Tabla 4-24. Opciones de Syslog disponibles a partir de ESXi 7.0 Update 1 (continuación)

<table>
<tr><th>Opción</th><th>Comando ESXCLI</th><th>Descripción</th></tr>
<tr><td>Syslog.global.logFilters</td><td>esxcli system syslog config logfilter [add | remove | set] ...</td><td>Especifica una o varias especificaciones de filtrado de registros. Cada filtro de registro debe estar separado por una barra vertical doble (||). El formato de los filtros de registro es: numLogs | ident | logRegexp. numLogs establece la cantidad máxima de entradas de registro para los mensajes de registro especificados. Una vez alcanzado este número, se filtran y se omiten los mensajes de registro especificados. ident especifica uno o más componentes del sistema para aplicar el filtro a los mensajes de registro que generan estos componentes. logRegexp especifica una frase que distingue mayúsculas de minúsculas con la sintaxis de la expresión regular Python para filtrar los mensajes de registro según su contenido.</td></tr>
<tr><td>Syslog.global.logFiltersEnable</td><td></td><td>Habilita el uso de filtros de registro.</td></tr>
<tr><td>Syslog.global.logLevel</td><td>esxcli system syslog config set --log-level=<str></td><td>Especifica el nivel de filtrado de registros. Debe cambiar este parámetro solo para solucionar problemas relacionados con el daemon de syslog. Puede utilizar los valores debug para el nivel más detallado, info para el nivel de detalle predeterminado, warning solo para advertencias o errores, o error solo para errores.</td></tr>
<tr><td>Syslog.global.msgQueueDropMark</td><td>esxcli system syslog config --queue-drop-mark=<long>)</td><td>Especifica el porcentaje de la capacidad de la cola de mensajes a partir del cual se descartan los mensajes.</td></tr>
<tr><td>Syslog.global.remoteHost.connectRetryDelay</td><td>esxcli system syslog config set --default-timeout=<long></td><td>Especifica el retraso antes de volver a intentar conectarse a un host remoto después de que se haya producido un error en un intento de conexión, en segundos.</td></tr>
</table>

Tabla 4-24. Opciones de Syslog disponibles a partir de ESXi 7.0 Update 1 (continuación)

Opción	Comando ESXCLI	Descripción
`Syslog.global.remoteHost.maxMsgLen`	`esxcli system syslog config set --remote-host-max-msg-len=<long>`	Para los protocolos TCP y SSL, este parámetro especifica la longitud máxima de una transmisión de Syslog antes de que se produzca truncamiento, en bytes. La longitud máxima predeterminada para los mensajes de host remoto es 1 KiB. Puede aumentar la longitud máxima del mensaje hasta 16 KiB. No obstante, aumentar este valor por encima de 1 KiB no garantiza que las transmisiones largas lleguen sin truncar a un recopilador de Syslog. Por ejemplo, cuando la infraestructura de syslog que emite un mensaje es externa a ESXi. Esta configuración no afecta al protocolo UDP. RFC 5426 establece la longitud máxima de transmisión de mensajes para el protocolo UDP en 480 bytes para IPV4 y 1180 bytes para IPV6. Debido a esta restricción, y debido a que la infraestructura de redes puede descartar de forma arbitraria los paquetes UDP, no se recomienda el uso de UDP para transmitir mensajes críticos de Syslog.
`Syslog.global.vsanBacking`	`esxcli system syslog config set --vsan-backing=<bool>`	Permite que los archivos de registro y el directorio de almacenamiento de registros de auditoría se coloquen en un clúster de vSAN. Sin embargo, si se habilita este parámetro, es posible que el host ESXi deje de responder.

Protocolos, formatos y marcos de mensajes de syslog de ESXi

A partir de ESXi 8.0, el servicio Syslog utiliza tres parámetros para definir mensajes y registros de auditoría: protocolo, formato y marcos.

Los protocolos compatibles son UDP, TCP y TLS (SSL). El formato de los mensajes de syslog se define mediante RFC 3164 o RFC 5424. Los marcos especifican cómo se encapsula un mensaje. Los marcos de mensajes encapsulados se definen como transparentes, también denominados octet_counting, o no transparentes, si un mensaje no está encapsulado. Los marcos transparentes garantizan que las nuevas líneas integradas en un mensaje no confundan a un recopilador de syslog. Los mensajes de syslog que se envían mediante el protocolo UDP se consideran incrustados en marcos de forma transparente; se espera que un recopilador de syslog comprenda esto y acepte la transmisión como un mensaje único.

RFC 3164 establece la longitud total máxima de un mensaje de syslog en 1024 bytes, mientras que RFC 5424 amplía este máximo a 2048 bytes.

La longitud máxima predeterminada para los mensajes de host remoto en ESXi es 1 KiB. Puede aumentar la longitud máxima del mensaje hasta 16 KiB. No obstante, aumentar este valor por encima de 1 KiB no garantiza que las transmisiones largas lleguen sin truncar a un recopilador de syslog. Por ejemplo, cuando la infraestructura de syslog que emite un mensaje es externa a ESXi.

Los mensajes de syslog que transmite vmsyslogd constan de datos estructurados, una lista de propiedades formateada de acuerdo con RFC 5424 y datos sin estructurar o de formato libre.

Cuando un mensaje supera la longitud máxima, ESXi 8.0 mitiga el mensaje e intenta conservar la mayor cantidad posible de datos estructurados.

Cuando se mitiga un mensaje, se agregan tres parámetros a los datos estructurados existentes o se crean datos estructurados que contengan estos parámetros: `msgModified`, `remoteHostMaxMsgLen` y `originalLen`.

El parámetro `msgModified` indica cómo afecta la mitigación al mensaje: solo datos estructurados, solo datos no estructurados o ambos.

El parámetro `remoteHostMaxMsgLen` especifica la longitud máxima del mensaje que ESXi puede controlar.

El parámetro `originalLen` especifica la longitud del mensaje antes de mitigarlo.

Opciones compatibles para protocolos, formatos y marcos de mensajes de syslog de ESXi:

Formatos	Marcos	UDP	TCP	SSL	Comentarios
Sin especificar	Sin especificar	Compatible RFC 5426	Compatible	Compatible	El formato de los mensajes cumple con RFC 3164, solo las marcas de tiempo tienen el formato RFC 3339. Los datos estructurados se anteponen a cada mensaje. El valor predeterminado de los marcos es no transparente con TCP o SSL (TLS) y las líneas nuevas integradas en datos estructurados podrían dañar los mensajes. Con UDP, los paquetes se incrustan en marcos.
Sin especificar	Non_transparent	Prohibido	Compatible	Compatible	El formato de los mensajes cumple con RFC 3164, solo las marcas de tiempo tienen el formato RFC 3339. Los datos estructurados se anteponen a cada mensaje. El valor predeterminado de los marcos es no transparente con TCP o SSL (TLS) y las líneas nuevas integradas en datos estructurados podrían dañar los mensajes.
Sin especificar	Octet_counting	Prohibido	Compatible RFC 6587	Compatible RFC 6587	El formato de los mensajes cumple con RFC 3164, solo las marcas de tiempo tienen el formato RFC 3339. Los datos estructurados se anteponen a cada mensaje.
RFC 5424	Sin especificar	Compatible RFC 5426	Compatible RFC 5425	Compatible RFC 5424	El formato de los mensajes cumple con RFC 5424. El valor predeterminado de los marcos es octet-counting con TCP o SSL (TLS). Con UDP, es posible que los marcos no se especifiquen de forma explícita.
RFC 5424	Non_transparent	Prohibido	No compatible	No compatible	No compatible porque las líneas nuevas integradas en datos estructurados podrían crear mensajes dañados.
RFC 5424	Octet_counting	Prohibido	Compatible RFC 5425	Compatible RFC 5425	El formato de los mensajes cumple con RFC 5424.

Formatos	Marcos	UDP	TCP	SSL	Comentarios
RFC 3164	Sin especificar	Compatible RFC 5426	Compatible	Compatible	El formato de los mensajes cumple con RFC 3164, solo las marcas de tiempo tienen el formato RFC 3339. Los datos estructurados se anteponen a cada mensaje. El valor predeterminado de los marcos es no transparente con TCP o SSL (TLS) y las líneas nuevas integradas en datos estructurados podrían dañar los mensajes. Con UDP, los paquetes se incrustan en marcos.
RFC 3164	Non_transparent	Prohibido	Compatible	Compatible	El formato de los mensajes cumple con RFC 3164, solo las marcas de tiempo tienen el formato RFC 3339. Los datos estructurados se anteponen a cada mensaje. El valor predeterminado de los marcos es no transparente con TCP o SSL (TLS) y las líneas nuevas integradas en datos estructurados podrían dañar los mensajes.
RFC 3164	Octet_counting	Prohibido	Compatible RFC 6587	Compatible RFC 6587	El formato de los mensajes cumple con RFC 3164, solo las marcas de tiempo tienen el formato RFC 3339. Los datos estructurados se anteponen a cada mensaje.

Formatos de archivo de registro

A partir de ESXi 8.0, el formato de los archivos de registro está estandarizado y se expresa en Augmented Backus-Naur Form (ABNF).

En ESXi 8.0, los archivos de registro se escriben directamente, desde un único servicio como VMX, o indirectamente, cuando los registros de un servicio se envían a syslog. Por ejemplo, VMX siempre escribe mensajes de registro en el archivo `vmware.log` de cada máquina virtual. Para ahorrar recursos del sistema, VMX no envía mensajes de registro al syslog. Por otro lado, en algunos archivos de registro que genera `vmsyslogd`, verá mensajes procedentes de varios programas, ya que el daemon de Syslog de ESXi crea y administra todos los archivos de registro y los mensajes a estos archivos desde varios servicios.

Formato de los mensajes de registro directos:

Parámetro	Valor
LOG-MSG	HEADER SP MSG
HEADER	TIMESTAMP SP SEVERITY SP THREAD-NAME SP OPID
TIMESTAMP	FULL-DATE T FULL-TIME (cumple con RFC 5424 con el requisito de formato y resolución UTC/GMT en milisegundos o más detallado cuando sea posible).
FULL-DATE	DATE-FULLYEAR - DATE-MONTH - DATE-MDAY
DATE-FULLYEAR	4DIGIT
DATE-MONTH	2DIGIT ; 01-12
DATE-MDAY	2DIGIT ; 01-28, 01-29, 01-30, 01-31 basado en mes/año
FULL-TIME	TIME-HOUR : TIME-MINUTE : TIME-SECOND[TIME-SECFRAC] Z
TIME-HOUR	2DIGIT ; 00-23
TIME-MINUTE	2DIGIT ; 00-59
TIME-SECOND	2DIGIT ; 00-59
TIME-SECFRAC	'.' 1*6DIGIT
SEVERITY	SEVERITY-STRING SEVERITY-VALUE [LINE-MARKER]
SEVERITY-STRING	Em/Al/Cr/Er/Wa/No/In/Db (los 8 niveles de gravedad especificados en RFC 5424 se abrevian de la siguiente manera: ■ Em: emergencia ■ Al: alerta ■ Cr: crítico ■ Er: error ■ Wa: advertencia ■ No: aviso ■ In: informativo ■ Db: depurar
SEVERITY-VALUE	(*DIGIT) (SEVERITY-VALUE es una expresión opcional del valor numérico asociado con SEVERITY-STRING. Esto permite que los niveles compatibles con un registrador se contraigan en las 8 cadenas requeridas sin perder información (p. ej., Db(5) - depurar, nivel 5).
LINE-MARKER	+ (LINE-MARKER se agrega a cada línea posterior generada a partir de un envío de varias líneas. Identifica los envíos de varias líneas y evita un ataque de seguridad por inserción de registros).
NILVALUE	- (Es posible que un solo programa de subprocesos no tenga un nombre de subproceso y que NILVALUE sea aceptable).
THREAD-NAME	NILVALUE / 1*32PRINTUSASCII (El componente (APP-NAME) está implícito cuando un solo programa escribe el archivo y no se necesita ningún campo de componente, solo el nombre del subproceso).
OPID	NILVALUE /1*128UTF-8-STRING
STRUCTURED-DATA	1*SD-ELEMENT

`SD-ELEMENT`	[SD-ID *(SP SD-PARAM)]
`SD-PARAM`	PARAM-NAME %d34 PARAM-VALUE %d34
`SD-ID`	SD-NAME
`PARAM-NAME`	SD-NAME
`PARAM-VALUE`	UTF-8-STRING ; caracteres '', '\' y ']' SE DEBEN evitar.
`SD-NAME`	1*32PRINTUSASCII ; excepto '', SP, ']', %d34 ()
`MSG`	[STRUCTURED-DATA SP] UTF-8-STRING

Formato de los archivos de registro que administra el servicio `vmsyslogd`:

Parámetro	Valor
`LOG-MSG`	HEADER SP MSG
`HEADER`	TIMESTAMP SP SEVERITY SP APP-NAME [PROC-IDENTIFIER] :
`APP-NAME`	1*32PRINTUSASCII
`PROC-IDENTIFIER`	[*DIGITS] ; el PID asociado con APP-NAME
`TIMESTAMP`	FULL-DATE T FULL TIME (resolución en milisegundos o más detallado cuando sea posible).
`FULL-DATE`	DATE-FULLYEAR - DATE-MONTH - DATE-MDAY
`DATE-FULLYEAR`	4DIGIT
`DATE-MONTH`	2DIGIT ; 01-12
`DATE-MDAY`	2DIGIT ; 01-28, 01-29, 01-30, 01-31 basado en mes/año
`FULL-TIME`	TIME-HOUR : TIME-MINUTE : TIME-SECOND[TIME-SECFRAC] Z
`TIME-HOUR`	2DIGIT ; 00-23
`TIME-MINUTE`	2DIGIT ; 00-59
`TIME-SECOND`	2DIGIT ; 00-59
`TIME-SECFRAC`	'.' 1*6DIGIT

SEVERITY-STRING	Em/Al/Cr/Er/Wa/No/In/Db (los 8 niveles de gravedad especificados en RFC 5424 se abrevian de la siguiente manera: ■ Em: emergencia ■ Al: alerta ■ Cr: crítico ■ Er: error ■ Wa: advertencia ■ No: aviso ■ In: informativo ■ Db: depurar
SEVERITY	SEVERITY-STRING PRI-STRING [LINE-MARKER]
PRIVAL	1*3DIGIT ; rango 0 .. 191 (MSG PRI; contiene los valores de gravedad y de instalación, ORed juntos)
PRI-STRING	(PRIVAL) (PRIVAL contiene los bits del mensaje PRI. Esto permite que se vea la funcionalidad del mensaje, así como los bits de gravedad en sí._
LINE-MARKER	+ (LINE-MARKER se agrega a cada línea posterior generada a partir de un envío de varias líneas. Identifica los envíos de varias líneas y evita un ataque de seguridad por inserción de registros).
STRUCTURED-DATA	1*SD-ELEMENT
SD-ELEMENT	[SD-ID *(SP SD-PARAM)]
SD-PARAM	PARAM-NAME %d34 PARAM-VALUE %d34
SD-ID	SD-NAME
PARAM-NAME	SD-NAME
PARAM-VALUE	UTF-8-STRING ; caracteres '', '\' y ']' SE DEBEN evitar.
SD-NAME	1*32PRINTUSASCII ; excepto '', SP, ']', %d34 ()
MSG	[STRUCTURED-DATA SP] UTF-8-STRING

Registros de auditoría

Los registros de auditoría de ESXi, con código de funcionalidad 13, cumplen con los formatos RFC 3164 y 5424, y se encuentran en la sección de datos estructurados. En el registro de auditoría, también encontrará información de seguimiento basada en eventos cuando esos datos están disponibles. Los registros de auditoría se almacenan en un formato especial, no en un archivo de registro normal. Puede acceder a los registros de auditoría de forma local mediante el programa `viewAudit` y la funcionalidad de administración de infraestructura virtual `FetchAuditRecords`. No lea, utilice ni edite un archivo de almacenamiento de registros de auditoría directamente. Los registros de auditoría almacenados en local cumplen con el formato de transmisión RFC 5424, donde `HOSTNAME` y `MSGID` son siempre `NILVALUE`.

Formatos de transmisión de mensajes de Syslog de ESXi

ESXi 8.0 asigna el formato a los mensajes de Syslog de acuerdo con RFC 3164 o RFC 5424.

La definición de los formatos de transmisión para RFC 3164 y RFC 5424 se encuentra en Augmented Backus-Naur Form (ABNF).

Formato de mensaje de transmisión RFC 3164

Parámetro	Valor
`SYSLOG-MSG`	HEADER SP MSG
`HEADER`	PRI TIMESTAMP SP HOSTNAME SP APP-NAME [PROC-IDENTIFIER] ":"
`PRI`	"<" PRIVAL ">"
`PRIVAL`	1*3DIGIT ; rango 0 .. 191 (MSG PRI; contiene los valores de gravedad y de instalación, ORed juntos)
`APP-NAME`	1*32PRINTUSASCII
`HOSTNAME`	1*255PRINTUSASCII
`PROC-IDENTIFIER`	"[" *DIGITS "]" ; el PID asociado con APP-NAME
`TIMESTAMP`	FULL-DATE "T" UTC-TIME (No establecer nunca un TIME-OFFSET)
`FULL-DATE`	DATE-FULLYEAR "-" DATE-MONTH "-" DATE-MDAY
`DATE-FULLYEAR`	4DIGIT
`DATE-MONTH`	2DIGIT ; 01-12
`DATE-MDAY`	2DIGIT ; 01-28, 01-29, 01-30, 01-31 basado en mes/año
`UTC-TIME`	TIME-HOUR ":" TIME-MINUTE ":" TIME-SECOND [TIME-SECFRAC] "Z"
`TIME-HOUR`	2DIGIT ; 00-23
`TIME-MINUTE`	2DIGIT ; 00-59
`TIME-SECOND`	2DIGIT ; 00-59
`TIME-SECFRAC`	"." 1*6DIGIT
`STRUCTURED-DATA`	1*SD-ELEMENT
`SD-ELEMENT`	"[" SD-ID *(SP SD-PARAM) "]"
`SD-PARAM`	PARAM-NAME "%d34 PARAM-VALUE %d34
`SD-ID`	SD-NAME
`PARAM-NAME`	SD-NAME
`PARAM-VALUE`	UTF-8-STRING ; Los caracteres '"', '' y ']' DEBEN tener caracteres de escape.
`SD-NAME`	1*32PRINTUSASCII ; excepto '', SP, ']', %d34 (")
`MSG`	[STRUCTURED-DATA SP] UTF-8-STRING

Formato de mensaje de transmisión RFC 5424

Parámetro	Valor
SYSLOG-MSG	HEADER SP STRUCTURED-DATA [SP MSG]
HEADER	PRI VERSION SP TIMESTAMP SP HOSTNAME SP APP-NAME SP PROCID SP MSGID
PRI	"<" PRIVAL ">"
PRIVAL	1*3DIGIT ; rango 0 .. 191; contiene datos de gravedad y funcionalidad
VERSION	NONZERO-DIGIT 0*2DIGIT
HOSTNAME	1*255PRINTUSASCII
APP-NAME	1*48PRINTUSASCII
NILVALUE	'-'
PROCID	NILVALUE | *DIGITS ; el PID asociado con APP-NAME
MSGID	NILVALUE
TIMESTAMP	FULL-DATE "T" UTC-TIME
FULL-DATE	DATE-FULLYEAR "-" DATE-MONTH "-" DATE-MDAY
DATE-FULLYEAR	4DIGIT
DATE-MONTH	2DIGIT ; 01-12
DATE-MDAY	2DIGIT ; 01-28, 01-29, 01-30, 01-31 basado en mes/año
UTC-TIME	TIME-HOUR ":" TIME-MINUTE ":" TIME-SECOND [TIME-SECFRAC] "Z"
TIME-HOUR	2DIGIT ; 00-23
TIME-MINUTE	2DIGIT ; 00-59
TIME-SECOND	2DIGIT ; 00-59
TIME-SECFRAC	"." 1*6DIGIT
STRUCTURED-DATA	NILVALUE / 1*SD-ELEMENT
SD-ELEMENT	"[" SD-ID *(SP SD-PARAM) "]"
SD-PARAM	PARAM-NAME " %d34 PARAM-VALUE %d34
SD-ID	SD-NAME
PARAM-NAME	SD-NAME
PARAM-VALUE	UTF-8-STRING ; Los caracteres '"', '' y ']' DEBEN tener caracteres de escape.
SD-NAME	1*32PRINTUSASCII ; excepto '', SP, ']', %d34 (")
MSG	MSG-UTF8

MSG-UTF8	BOM UTF-8-STRING
BOM	%xEF.BB.BF

Configurar el filtrado de registros en hosts ESXi

Las capacidades de filtrado de registros permiten modificar la directiva de registro del servicio de Syslog que se ejecuta en un host ESXi.

A partir de vSphere 7.0 Update 2, puede agregar filtros de registro y habilitar el filtrado de registros mediante ESXCLI. Un filtro de registro, una vez establecido, permanece operativo hasta que se elimina, incluso después de reiniciar ESXi.

Los filtros de registro afectan a todos los eventos de registro que procesa el servicio de `vmsyslogd` del host ESXi, ya sea que se registren en un directorio de registro o en un servidor syslog remoto.

Debe habilitar la capacidad de filtrado de registros y volver a cargar el daemon de Syslog para activar los filtros de registros en el host ESXi.

Los comandos ESXCLI para configurar los filtros de registro siguen este patrón: `esxcli system syslog config logfilter {cmd} [cmd options]`.

Por ejemplo, para obtener la lista de filtros de registro disponibles, ejecute el siguiente comando: `[root@xxx-xx-dhcp-xx-xx:~] esxcli system syslog config logfilter list`.

Utilice el comando `set` para activar o desactivar el filtrado de registros: `[root@xxx-xx-dhcp-xx-xx:~] esxcli system syslog config logfilter set`.

Utilice el comando `add` para agregar un filtro de registro y el comando `remove` para eliminarlo.

Utilice el comando `get` para determinar si el filtrado de registros está habilitado.

Un filtro de registro se especifica mediante tres componentes y utiliza la siguiente sintaxis: `numLogs | ident | logRegexp`.

Parámetro	Descripción
`numLogs`	Especifica el número de coincidencias de la expresión regular de Python logRegexp que se permitirá antes de que comience el filtrado.
`ident`	La cadena `ident` es la forma en que una aplicación se identifica en la instalación de syslog. El filtro de `logRegexp` debe estar asociado a la misma aplicación. Para encontrar la cadena `ident` de una aplicación, inspeccione los archivos de registro en `/var/run/log`. El tercer campo de cada archivo de registro comienza con la cadena `ident` y termina con `[`.
`logRegexp`	Expresión regular de Python que identifica los mensajes que desea filtrar.

Por ejemplo, para filtrar todos los mensajes del daemon de hostd que contienen la palabra "mark" después de la décima aparición, utilice el siguiente comando: `esxcli system syslog config logfilter add --filter="10|Hostd|mark"`.

Para eliminar el filtro de registro, utilice el comando `esxcli system syslog config logfilter remove --filter="10|Hostd|mark"`.

Para obtener más información, consulte Opciones de syslog de ESXi.

Requisitos previos

Puede crear filtros de registros para reducir la cantidad de entradas repetidas en los registros de ESXi y agregar a la lista de no permitidos eventos de registros específicos en su totalidad.

Instale ESXCLI. Consulte *Introducción a ESXCLI*. Para solucionar problemas, ejecute los comandos de `esxcli` en ESXi Shell.

Configurar el nivel de aceptación del perfil de imagen de host

El nivel de aceptación del perfil de imagen del host determina qué paquetes de instalación de vSphere (VIB) se aceptan para la instalación.

Las firmas de VIB se comprueban y se aceptan para la instalación según una combinación del nivel de aceptación de VIB y nivel de aceptación del perfil de imagen del host. Los VIB se etiquetan con un nivel de aceptación que depende del estado de la firma.

Consulte Trabajar con niveles de aceptación.

Requisitos previos

Privilegios requeridos: **Host.Configuration.Security Profile** and **Host.Configuration.Firewall**

Procedimiento

1 Desde vSphere Client, conéctese a vCenter Server.

2 Seleccione el host en el inventario.

3 Haga clic en la pestaña **Configurar**.

4 En Sistema, seleccione **Perfil de seguridad**.

5 Desplácese hacia abajo hasta Nivel de aceptación del perfil de imagen del host y haga clic en **Editar**.

6 Seleccione el nivel de aceptación y haga clic en **Aceptar**.

Tabla 4-25. Niveles de aceptación del perfil de imagen del host

Nivel de aceptación del perfil de imagen del host	Niveles aceptados de los VIB
Certificado por VMware	Certificado por VMware
Aceptado por VMware	Certificado por VMware, Aceptado por VMware

Tabla 4-25. Niveles de aceptación del perfil de imagen del host (continuación)

Nivel de aceptación del perfil de imagen del host	Niveles aceptados de los VIB
Creado por los partners	Certificado por VMware, Aceptado por VMware, Creado por los partners
Creado por la comunidad	Certificado por VMware, Aceptado por VMware, Creado por los partners, Creado por la comunidad

Quitar todos los paquetes personalizados en ESXi

Después de agregar paquetes personalizados, puede que se decida quitarlos.

Requisitos previos

Antes de quitar paquetes personalizados, apague o migre las máquinas virtuales en ejecución fuera del host ESXi.

Procedimiento

1 Reinicie el host ESXi.

2 En la consola directa, seleccione **Quitar extensiones personalizadas** y presione F11 para confirmar.

3 Reinicie el host.

Resultados

Se quitan todos los paquetes personalizados.

Modificar los archivos de configuración de ESXi

Los archivos de configuración de ESXi se pueden modificar en el almacén de configuración de ESXi (ConfigStore) mediante la herramienta `/bin/configstorecli`.

El objetivo de la herramienta ESXi Shell `configstorecli`, introducida en ESXi 7.0 Update 1, es administrar todas las configuraciones de un host ESXi de forma centralizada, en lugar de utilizar diferentes métodos y una variedad de archivos de configuración.

Para obtener más información sobre cómo administrar ConfigStore, consulte los artículos de la base de conocimientos 82227 y 93720 de VMware.

Desactivar la compatibilidad con caracteres no ASCII en ESXi

Puede desactivar la compatibilidad con caracteres que no sean ASCII para los archivos de máquinas virtuales y los nombres de directorios mediante dos métodos, según la versión de ESXi.

De forma predeterminada, ESXi admite el uso de caracteres no ASCII para los nombres de directorios y archivos de máquinas virtuales.

Si necesita desactivar la compatibilidad con caracteres que no sean ASCII, para ESXi 7.0 Update 2 y versiones posteriores, consulte los artículos de la base de conocimientos 82227 y 93720 de VMware.

Antes de ESXi 7.0 Update 2, puede desactivar esta compatibilidad si modifica el archivo `/etc/vmware/hostd/config.xml` con estos pasos:

Procedimiento

1 Mediante un editor de texto, abra el archivo `/etc/vmware/hostd/config.xml` para el host ESXi.

2 En la etiqueta `<config></config>`, agregue el código siguiente.

```
<g11nSupport>false</g11nSupport>
```

3 Guarde y cierre el archivo.

4 Reinicie el host.

Una vez que desactive esta compatibilidad, podrá seguir introduciendo caracteres no ASCII en los nombres de las máquinas virtuales. Las interfaces de usuario de vSphere muestran los nombres de las máquinas virtuales en caracteres no ASCII, pero ESXi convierte los nombres del archivo en cuestión y los nombres de directorios en cadenas ASCII.

Restablecer la configuración del sistema

Si tiene problemas para determinar el origen de un problema con su host ESXi, puede restablecer la configuración del sistema.

Los cambios en la configuración del sistema pueden estar relacionados con diferentes problemas, incluidos los problemas de conectividad con la red y dispositivos. Restablecer la configuración del sistema podría resolver estos problemas. Si restablecer la configuración del sistema no resuelve el problema, puede descartar los cambios en la configuración realizados desde la configuración inicial como el origen del problema.

Cuando restablezca la configuración, el software anula todos los cambios en la configuración, elimina la contraseña de la cuenta de administrador (raíz) y reinicia el host. También podrían eliminarse los cambios en la configuración realizados por el proveedor del hardware, como la configuración de direcciones IP y la configuración de licencias.

El restablecimiento de la configuración no elimina las máquinas virtuales del host ESXi. Después de restablecer los valores predeterminados de configuración, las máquinas virtuales no aparecen visibles, pero puede volver a lograr que estén visibles reconfigurando el almacenamiento y volviendo a registrar las máquinas virtuales.

Precaución Cuando restablezca los valores predeterminados de configuración, los usuarios que están accediendo al host pierden conectividad.

Requisitos previos

Antes de restablecer la configuración, realice una copia de seguridad de su configuración de ESXi en caso de que desee restaurar su configuración.

Procedimiento

1 Realice una copia de seguridad de la configuración mediante el cmdlet de PowerCLI `Get-VMHostFirmware`.

2 Desde la consola directa, seleccione **Restablecer la configuración del sistema** y presione Intro.

3 Presione F11 para confirmar.

Resultados

El sistema se reiniciará después de que la configuración se restablezca a los valores predeterminados.

Después de instalar y configurar ESXi

Después de instalar y configurar ESXi, puede usar la administración de hosts mediante varias interfaces, otorgar licencias a los hosts y realizar una copia de seguridad de la configuración.

Una vez que ESXi está instalado y configurado, puede administrar el host mediante vSphere Client y vCenter Server, aplicar una licencia al host y crear una copia de seguridad de la configuración de ESXi. También puede usar VMware Host Client para conectarse directamente al host ESXi y administrarlo. Para obtener información sobre cómo instalar y utilizar VMware Host Client, consulte *Administrar un host único de vSphere*.

Nota Cuando instale un host ESXi independiente con TMP activado que no esté conectado a una instancia de vCenter Server, cree una copia de seguridad de la clave de recuperación de la configuración de ESXi. Para obtener la clave de recuperación, ejecute el comando `esxcli system settings encryption recovery list` en el host ESXi y anótela. Es posible que el host no pueda completar el arranque debido a problemas relacionados con el cifrado de la configuración del host y, en tales casos, puede restaurar la configuración del host utilizando la clave de recuperación y ejecutando el proceso de recuperación de la configuración.

Para obtener información sobre prácticas recomendadas y sugerencias de VMware, consulte Prácticas recomendadas para la configuración segura de ESXi.

Licencias de hosts ESXi

Después de instalar ESXi, el software ofrece un período de evaluación de 60 días durante el cual se puede explorar el conjunto completo de funciones de vSphere que se obtienen con una licencia de vSphere Enterprise Plus. Debe asignar al host una licencia adecuada antes de que caduque el período de evaluación.

Los hosts ESXi incluyen licencias de vSphere que proporcionan capacidad por CPU. Para proporcionar las licencias correctas a los hosts, debe asignarles una licencia de vSphere que cuente con capacidad de CPU suficiente para abarcar todos los CPU de los hosts. La licencia debe admitir todas las funciones que utilizan los hosts. Por ejemplo, si los hosts están conectados a vSphere Distributed Switch, debe asignarles una licencia que incluya la característica vSphere Distributed Switch.

Puede emplear uno de los métodos siguientes para asignar licencias a los hosts ESXi:

- Asignar licencias a varios hosts a la vez mediante la función de administración de licencias de vSphere Client. Los hosts deben estar conectados a un sistema vCenter Server. Para obtener más información, consulte *Administrar vCenter Server y hosts*.
- Configurar licencias masivas mediante los comandos de PowerCLI. Las licencias masivas funcionan para todos los hosts ESXi, pero son especialmente útiles para los hosts aprovisionados con Auto Deploy. Consulte Configurar licencias masivas
- Otorgue licencias a hosts ESXi individuales mediante el uso de una conexión directa con VMware Host Client. Para obtener información sobre cómo asignar una clave de licencia para un host ESXi, consulte *Administrar un host único de vSphere*.

Registro de la clave de licencia de un host ESXi

Si no es posible acceder a un host o arrancarlo, deberá tener un registro de su clave de licencia. Puede escribir la clave de licencia y pegarla con cinta en el servidor o colocar la clave de licencia en una ubicación segura. Puede acceder a la clave de licencia desde la interfaz de usuario de la consola directa o vSphere Client.

Ver las claves de licencia de los hosts ESXi desde vSphere Client

Puede ver las claves de licencia de los hosts que están conectados a un sistema vCenter Server a través de vSphere Client.

Procedimiento

1. En vSphere Client, seleccione **Administración**.
2. En Licencias, seleccione **Licencias**.
3. En la pestaña **Activos**, seleccione **Hosts**.
4. En la columna Licencia, haga clic en una licencia.

Resultados

Verá información sobre la licencia, como su uso y la clave de licencia.

Acceder a la clave de licencia de ESXi desde la consola directa

Si tiene acceso físico al host o acceso remoto a la consola directa, puede utilizar la consola directa para acceder a la clave de licencia de ESXi.

Procedimiento

- En la consola directa, seleccione **Ver información de soporte**.

  La clave de licencia aparece con el formato XXXXX-XXXXX-XXXXX-XXXXX-XXXXX, etiquetada como Número de serie de la licencia.

  Nota También aparece el número de serie del equipo físico, etiquetado como Número de serie. No confunda la clave de licencia con el número de serie del equipo físico.

Ver registros del sistema

Los registros del sistema proporcionan información detallada sobre los eventos operativos del sistema.

Procedimiento

1 En la consola directa, seleccione **Ver registros del sistema**.

2 Presione la tecla numérica que corresponda para ver un registro.

   Si agrega el host a vCenter Server, aparecen los registros de vCenter Server Agent (vpxa).

3 Presione Intro o la barra espaciadora para desplazarse por los mensajes.

4 Realice una búsqueda de expresiones regulares.

   a Presione la tecla de barra diagonal (/).

   b Escriba el texto que desea buscar.

   c Presione Intro.

   El texto que se encontró aparece resaltado en la pantalla.

5 Presione q para volver a la consola directa.

Pasos siguientes

Consulte también Configurar Syslog en hosts ESXi.

Solución de problemas de arranque de ESXi

5

En los temas de solución de problemas de arranque de ESXi, se proporcionan soluciones para los problemas que se pueden enfrentar al arrancar ESXi.

Lea los siguientes temas a continuación:

El host se detiene inesperadamente durante el arranque cuando comparte un disco de arranque con otro host

Cuando dos hosts o más, ya sean físicos o virtuales, arrancan desde el mismo LUN o desde el mismo disco físico compartido, no pueden usar la misma partición temporal.

Problema

El host se detiene en el arranque cuando comparte un disco de arranque con otro host.

Causa

Dos hosts ESXi o más pueden compartir el mismo LUN o el mismo disco físico. Cuando hay dos hosts de este tipo que, además, tienen configurada la misma partición temporal, cualquiera de los dos hosts puede experimentar un error en el arranque.

Solución

1 Establezca los hosts para que arranquen de manera secuencial y, a continuación, arránquelos.

   Esta configuración permite iniciar los hosts de manera tal que pueda cambiar la partición temporal para uno de ellos.

2 Desde vSphere Client, conéctese a vCenter Server.
3 Seleccione el host en el inventario.
4 Haga clic en la pestaña **Configurar**.
5 En Sistema, seleccione **Configuración avanzada del sistema**.

6 Seleccione **ScratchConfig**.

El cuadro de texto **ScratchConfig.CurrentScratchLocation** muestra la ubicación actual de la partición desde cero.

7 En el cuadro de texto **ScratchConfig.ConfiguredScratchLocation**, introduzca una ruta de acceso de directorio que sea exclusiva para este host.

Por ejemplo, **`/vmfs/volumes/`*`DatastoreUUID`*`/`*`DatastoreFolder`***.

8 Reinicie el host para que se apliquen los cambios.

El host no arranca después de instalar ESXi en modo UEFI

Después de instalar ESXi en un equipo host en modo UEFI, la máquina podría generar un error al arrancar.

Problema

Al instalar o actualizar ESXi, el instalador intenta crear una opción de arranque UEFI denominada `VMware ESXi` y convertirla en la opción de arranque predeterminada. Cuando se reinicia después de instalar ESXi, es posible que se produzca un error en el reinicio. Este problema viene acompañado de un mensaje de error similar a `No hay dispositivo de arranque disponible.`

Causa

- Cuando el instalador crea la opción de arranque UEFI, se produce un problema al escribir en la NVRAM de la placa base del host.
- El firmware del host no reconoce el intento de establecer la opción de arranque UEFI como la opción de arranque inicial, o bien el firmware anula el orden de arranque.
- El disco de arranque tiene una tabla de particiones MBR o MSDOS. Debido a una limitación técnica, la opción de arranque UEFI solo se crea para una tabla de particiones GUID Partition Table (GPT).

Nota El firmware UEFI intenta cargar la imagen de arranque desde la partición del sistema EFI, que está basada en FAT, en el disco. El arranque desde la partición del sistema EFI solo funciona si el disco se establece mediante un GPT. Si el disco de arranque tiene una tabla de particiones MBR o MSDOS, se produce un error en el arranque UEFI. No se puede agregar una entrada de arranque para MBR. Si el disco está totalmente consumido por ESXi, no se puede convertir a GPT y debe arrancar en modo BIOS heredado.

Solución

1 Mientras se muestra el mensaje de error en la pantalla, abra el menú de opciones de arranque. Dependiendo del sistema, el menú de opciones de arranque puede abrirse con un método abreviado de teclado, en el menú del BIOS o en una interfaz de BMC, iLO o iDRAC.

2 Compruebe si existe una opción de arranque `VMware ESXi` e intente arrancar desde ella. Si el arranque se realiza correctamente, cambie el orden de arranque y establezca `VMware ESXi` como la opción de primer arranque.

3 Si el problema no se resuelve, seleccione una opción similar a **Agregar opción de arranque**.

La redacción y la ubicación de la opción podría variar, según el sistema.

4 Seleccione el archivo `\EFI\BOOT\BOOTx64.EFI` en el disco en el que instaló ESXi.

5 Cambie el orden de arranque de manera que el host arranque desde la opción que haya agregado.

6 Desinstalar un host ESXi

Si no desea que el servidor sea un host ESXi, puede desinstalar el equipo host ESXi.

Procedimiento

1 Quite los almacenes de datos de VMFS en los discos internos para que los discos internos ya no se configuren para almacenar máquinas virtuales.

2 Cambie la configuración de arranque en el BIOS para que el host ya no arranque en ESXi.

   Si instaló ESXi en modo UEFI, elimine la opción de arranque `VMware ESXi` o cualquier otra opción que se haya creado manualmente.

3 Instale otro sistema operativo en su lugar.